Fundamentos de Matemáticas

Carlos Alberto Banquet Brango

Sergio Miguel Avilez Ortiz

Departamento de Matemáticas y Estadística

Facultad de Ciencias Básicas

Universidad de Córdoba, Colombia

2015

Prefacio

Este libro está diseñado para ser desarrollado en el primer año de carrera de los programas de Matemáticas o Estadística, en los cursos que usualmente son llamados Fundamentos de Matemáticas. La idea de escribir este texto surgió como respuesta a la falta de un único texto en Castellano que abarcara todos los temas que se estudian en los cursos antes mencionados. Este libro está basado en las notas de clases que se han usado durante más de cinco años en los cursos de Fundamentos de Matemáticas I y II, de los programas de Matemáticas y Estadística de la Universidad de Córdoba. El objetivo principal de este libro es dar la fundamentación necesaria al estudiante para afrontar cursos de Matemáticas o Estadística más avanzados, como lo son la Teoría de Números, Análisis Matemático, Teoría de Grupos, Probabilidad e Inferencia Estadística.

Para el estudio de este libro el estudiante no necesita ningún pre-requisito especial, solo los cursos usuales de matemáticas desarrollados en la secundaria. Con el objetivo que el lector comprenda con más facilidad los temas abordados, se han hecho una gran cantidad de ejemplos en cada capítulo y una lista de ejercicios bastante grande, la cual le permitirá al estudiante tener una mejor oportunidad de prácticar las técnicas y conceptos explicados.

El libro consta de diez capítulos, los cuales pueden ser desarrollados en un año, los cinco primeros en un semestre y el resto en el siguiente. En el primer capítulo se hace un estudio de la lógica desde un punto de vista informal, con el objetivo que cualquier egresado de la secundaria lo pueda entender sin inconvenientes. El segundo capítulo aborda el estudio de los metodos de pruebas, se dan muchos ejemplos sobre pruebas directas, por contradicción, por absurdo, por casos y demás variaciones importantes. En el tercer capítulo de estudian las clases y conjuntos, de nuevo desde un punto de vista intuitivo. En esta parte del libro el estudiante se afianza en el uso de los metodos de pruebas y se establecen las propiedades más importantes de la Teoría de Conjuntos. El cuarto capítulo está dedicado al estudio de las funciones, se define la imagen directa e inversa, inyectividad, sobreyectividad, biyectividad, composición e inversas, y se establecen sus propiedades más importantes. En el quinto capítulo se estudian las relaciones, es un estudio sucinto de la propiedades importantes de éstas. La idea central es introducir las relaciones de equivalencia y el concepto de partición.

El abordaje de los conceptos del capítulo seis hasta el diez es un poco más formal. En el sexto capítulo se estudian los números reales con una construcción axiomatica, el objetivo es demostrar las propiedades más relavantes de una forma rápida. El séptimo capítulo es dedicado al estudio de los campos ordanados completos, se introduce el Axioma de Completez y sus consecuencias más importantes. El octavo capítulo tiene por objeto el análisis de la cardinalidad de conjuntos, se definen

conjuntos finitos, infinitos, numerables, contables y no-contables, y se establecen las propiedades relevantes de éstos. Una introducción a los números complejos es hecha en el noveno capítulo, objetivo primordial de esta parte del libro es preparar al alumno para los curso de Variable Compleja y Álgebra Abstracta. Finalmente, en el decimo capítulo de hace una breve presentación sobre Polinomios definidos en los número reales y complejos.

Como es bien sabido por la comunidad matemática, lo contenidos abordados en este texto son clásicos y son los que debe conocer un matemático en sus primeros semestres de fomación, sin embargo el abordaje dado en este libro es moderno y práctico, debido a que permite un rápido entendimiento de los conceptos y el lenguaje de la matemática actual.

Índice general

Prefacio **ii**

1. Lógica Informal **1**

1.1. Afirmaciones 2

1.2. Relaciones entre Afirmaciones. 6

1.3. Argumentos Válidos. 10

1.4. Cuantificadores. 16

1.5. Ejercicios 22

2. Estrategias de Prueba **28**

2.1. Pruebas en Matemáticas. 28

2.2. Pruebas Directas. 29

2.3. Pruebas por Contrarrecíproco y Contradicción. 32

2.4. Método de Casos y Pruebas de "si y sólo si". 33

2.5. Cuantificadores en Teoremas. 37

2.6. Escribiendo Matemáticas 41

2.7. Ejercicios 42

3. Clases y Conjuntos. **46**

3.1. Definiciones Básicas. 47

3.2. Operaciones entre Clases. 49

3.3. Producto Cartesiano. 53

3.4. Familias Indexadas de Clases. 55

3.5. Ejercicios 58

4. Funciones. 63

4.1. Funciones. 63

4.2. Imagen e Imagen Inversa. 66

4.3. Composición de Funciones y Funciones Inversas. 68

4.4. Inyectividad, Sobreyectividad y Biyectividad. 70

4.5. Ejercicios 73

5. Relaciones. 79

5.1. Conceptos Fundamentales. 79

5.2. Relaciones de Equivalencia 83

5.3. Ejercicios 85

6. El Sistema de Números Reales 88

6.1. Axiomas de un Campo Ordenado 88

6.2. Operaciones Aritméticas en un Campo 92

6.3. Desigualdades en un Campo Ordenado y Valor Absoluto 94

6.4. Números Naturales e Inducción 98

6.5. Enteros y Racionales. 106

6.6. Ejercicios 107

7. Conjuntos Acotados en un Campo Ordenado. 111

7.1. Aplicaciones del Axioma de Completez. 114

7.2. Algunos Resultados Adicionales 116

7.3. Raíces. Números Irracionales 117

7.4. Potencias con Exponente Real Arbitrario 119

7.5. Sistema Ampliado de Números Reales 120

7.6. Ejercicios 121

8. Cardinalidad. 125

8.1. Conjuntos Equipotentes; Conjuntos Finitos 125

8.2. Conjuntos Infinitos y Contables 131

8.3. Conjuntos no Contables 134

8.4. Ejercicios 136

9. Los Números Complejos 139

9.1. Álgebra de los Números Complejos 139

9.2. Complejos Conjugados. Módulo de Complejos 141

9.3. Raíces Cuadradas de un Complejo 143

9.4. Forma Trigonométrica de un Complejo 144

9.5. Fórmula de Moivre 146

9.6. Resolución de la Ecuación $x^n - z = 0$ 147

9.7. Representación Geométrica de las Raíces 148

9.8. Las Raíces n-ésimas de la Unidad. 149

9.9. Ejercicios 150

10.Polinomios 153

10.1. Definiciones Básicas 153

10.2. Ecuaciones Polinomiales de Segundo Grado 154

10.3. Factorización de Polinomios 155

10.4. Polinomios Sobre $\mathbb{R}$ 159

10.5. División Sintética 161

10.6. Ejercicios 162

Índice alfabético **165**

Capítulo 1

Lógica Informal

La lógica es un área de la matemática que se encarga de estudiar los principios formales del razonamiento o la inferencia correcta. En un nivel elemental, la lógica proporciona reglas y técnicas para determinar si es o no válido un argumento dado. El razonamiento lógico es usado en matemáticas para hacer demostraciones, en computación para determinar si un programa es correcto, en ciencias naturales sirve para obtener conclusiones de los experimentos realizados y en general en la vida cotidiana para resolver una amplia variedad de problemas. La lógica tradicional como parte de la Filosofía es una de las disciplinas científicas más antiguas de la humanidad, cuyo origen se remonta a los trabajos de Aristóteles y es la raíz de lo que en la actualidad se llama Lógica Filosófica. En contraste, la Lógica Matemática es una disciplina relativamente joven y en general se reconoce a Gottfried Leibniz como el primer lógico matemático, pero fueron George Boole y Augustus de Morgan que por primera vez presentaron un sistema lógico en la forma como lo conocemos hoy. El trabajo de Boole y De Morgan fue retomado, mejorado y llevado a otros niveles por brillantes matemáticos y filósofos tales como Charles Peirce, Gottlob Frege, Giuseppe Peano, Alfred Whitehead, Bertrand Russell, David Hilbert, Kurt Gödel, Alan Turing, Alfred Tarski y otros. Vale la pena mencionar el trabajo de Kurt Gödel, quien es considerado el lógico más importante del siglo veinte. El más célebre de sus resultados es el Teorema de Incompletitud, que de manera bastante informal, establece que para todo sistema axiomático recursivo auto-consistente lo suficientemente poderoso como para describir la aritmética de los números naturales (la aritmética de Peano), existen proposiciones verdaderas sobre los naturales que no pueden demostrarse a partir de los axiomas. Para demostrar este teorema desarrolló una técnica denominada en este momento como numeración de Gödel, la cual codifica expresiones formales como números naturales. Los resultados de Gödel son fundamentales en la actualidad para las ciencias teóricas de la computación. El desarrollo de la Lógica matemática nos llevo a novedosos campos de aplicación que han mejorado de manera radical nuestra vida, por ejemplo el sistema creado por Boole redujo a argumentos lógicos las permutaciones de tres operadores básicos algebraicos: y, o y no. A causa del desarrollo del álgebra de Boole, Boole es considerado por muchos como el padre de la teoría de la informática. Por su parte, Alan Turing proporcionó una influyente formalización de los conceptos de algoritmo y computación: la máquina de Turing. También, formuló su propia versión de la hoy ampliamente aceptada Tesis de Church-Turing, la cual postula que cualquier modelo computacional existente tiene las mismas capacidades algorítmicas, o

un subconjunto, de las que tiene una máquina de Turing. Por todo esto Turing es considerado uno de los padres de la ciencia de la computación siendo el precursor de la informática moderna. Otro personaje muy importante en la historia de la lógica es John von Neumann, conocido como el genio multidisciplinar por sus contribuciones en Física Cuántica, Análisis Funcional, Teoría de Conjuntos, Ciencias de la Computación, Economía, Análisis Numérico, Cibernética, Hidrodinámica, Estadística y muchos otros campos. Von Neumann hizo completamente satisfactoria la teoria axiomática de conjuntos y la siguiente pregunta era si aquella era o no definitiva y no estaba sujeta a mejoras. La contundente respuesta negativa la dio Kurt Gödel, cuando en septiembre de 1930 en el histórico Congreso de Königsberg, anunció su famoso primer Teorema de la Incompletitud. La arquitectura utilizada en casi todos los computadores es llamada de Von Neumann por su publicación del concepto. Virtualmente, cada computador personal, microcomputador, minicomputador y supercomputador es una máquina de von Neumann. También creó el campo de los autómatas celulares sin computadores, construyendo los primeros ejemplos de autómatas autorreplicables con lápiz y papel.

En este capítulo estaremos un poco alejados de la teoría moderna de la lógica, lo que haremos será apenas lo suficiente para entender como se hace una prueba rigurosa y lo desarrollaremos de forma informal. El objetivo es explicar que son afirmaciones bien formadas y argumentos válidos, éstas dos nociones nos permitirán establecer y probar teoremas. Comencemos definiendo el elemento principal de trabajo de este capítulo, las afirmaciones.

1.1. Afirmaciones

Las afirmaciones son los bloques fundamentales en la construcción de la matemática, pero tenemos que tener bien claro que frases serán consideradas como afirmaciones.

Definición 1.1 (Afirmación)**.** *Intuitivamente una afirmación es algo que expresamos (en forma oral, escrita o de cualquier otra manera) y que en un contexto dado es inequívocamente cierto o falso.*

Existen algunas paradojas, tales como "Esta afirmación es falsa" la cual no puede ser cierta o falsa. Si creemos que es cierta entonces por su contenido sería falsa y si fuese falsa, tendríamos que la afirmación es verdadera. Nosotros no consideraremos las paradojas como afirmaciones.

Ejemplo 1.2. *"Bogotá es la capital de Colombia" y "Marie Curie nació el 7 de noviembre de 1867". Ambas son afirmaciones. De la primera no tenemos duda si es verdadera o falsa y de la segunda no hay certeza, sin embargo, también es una afirmación y no es necesario estar en la capacidad de saber personalmente la respuesta.*

Ejemplo 1.3. *"Viajar en la noche", "¿Qué hora es?" y "mirar televisión". No son afirmaciones. De éstas no se puede decir que sean verdaderas o falsas.*

Ejemplo 1.4. *"Todo número entero par mayor que 2 puede escribirse como la suma de dos números primos" es una afirmación la cual hasta el día de hoy no ha sido resuelta y por tanto no sabemos si es cierta o falsa, pero sigue siendo una afirmación. De hecho es una de las conjeturas más importantes en Teoría de Números, propuesta por Christian Goldbach en 1742 (Esto quiere decir que la humanidad lleva mas de 270 años sin resolverla). Esta conjetura ha sido investigada por muchas*

personas y ha sido comprobada computacionalmente para todos los números enteros pares menores que 10^{18}.

Toda afirmación es verdadera o falsa y no hay una afirmación que sea verdadera y falsa al mismo tiempo. Esta suposición la llamamos la **Ley del Medio Excluido**. En este punto es bueno recordar que existen "lógicas polivalentes" donde este principio no es aceptado. Es decir que no se puede mostrar que una afirmación es verdadera probando que su negación es falsa, pues pueden existir otros valores de verdad además de los tradicionales verdadero y falso. Sin embargo, en este libro aceptaremos la Ley de Medio Excluido y una consecuencia para nuestro contexto será que si una afirmación no es falsa tendrá que ser verdadera.

A partir de una o varias afirmaciones podemos construir otras afirmaciones. Teniendo como base las afirmaciones P: "Bogotá es la capital de Colombia", Q: "Marie Curie nació el 7 de noviembre de 1867 ", podemos construir nuevas afirmaciones, por ejemplo P y Q: "Bogota es la capital de Colombia y Marie Curie nació el 7 de noviembre de 1867", P o Q: "Bogotá es la capital de Colombia o Marie Curie nació el 7 de noviembre de 1867".

Operaciones Básicas.
Las palabras "y", "o", "no", "si,. . . , entonces", "si y sólo si", nos permitirán hacer nuevas afirmaciones y además, conociendo los valores de verdad de las afirmaciones que componen la nueva afirmación, podremos deducir el valor de verdad de ésta. Dichas palabras tienen una notación especial y su sentido en matemáticas es preciso, como vemos a continuación.

1. **Conjunción:** $\wedge$ (Corresponde al **"y"** del lenguaje común). Sean P y Q afirmaciones. La afirmación $P \wedge Q$ se lee "P y Q" e intuitivamente es verdadera si ambas son verdaderas y falsa si alguna de ellas es falsa, pero su definición precisa se consigna en la siguiente tabla, que llamamos tabla de verdad.

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

 En el lenguaje común la palabra **"y"** podría tener otros significados, sin embargo para nosotros el significado es el que nos da la tabla dada arriba.

2. **Disyunción:** $\vee$ (Corresponde al **"o"** del lenguaje común). La afirmación $P \vee Q$ se lee "P o Q", intuitivamente $P \vee Q$ es verdadero si cualquiera de las dos afirmaciones lo es o si ambas lo son. De forma más precisa:

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Este es un "o" inclusivo y no exclusivo. En el lenguaje coloquial muchas veces no se permite que ambas sean verdaderas. Por ejemplo: Después del almuerzo duermo o voy a trabajar. En la afirmación anterior dada en lenguaje común uno entiende que no hará las dos cosas después del almuerzo. Aquí el "o" es exclusivo, pero en el lenguaje matemático el "o" que se usa es el inclusivo.

3. **Negación:** $\neg$ (Corresponde al **"no"** del lenguaje común). La afirmación $\neg P$ se lee "no P", intuitivamente $\neg P$ es falso cuando P es verdadero y $\neg P$ es verdadero cuando P no lo es. La definición precisa de la negación es:

P	$\neg P$
V	F
F	V

Por ejemplo, si P: Bogotá es la capital de Colombia, su negación será $\neg P$: Bogotá no es la capital de Colombia.

4. **Condicional:** $\rightarrow$ (Corresponde al **"si,..., entonces..."** del lenguaje común). La afirmación $P \rightarrow Q$ se lee "Si P, entonces Q". Intuitivamente, es verdadera si nunca ocurre que P sea verdadera y Q sea falsa. La definición precisa es:

P	Q	$P \rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

$P \rightarrow Q$ se puede escribir $Q \leftarrow P$. Usualmente a P lo llamamos el **antecedente** y a Q el **consecuente**. Así pues, los dos últimos renglones de la tabla los interpretamos así: Si el antecedente es falso, cualquier cosa puede ocurrir con el consecuente y al final toda la afirmación sera verdadera. $P \rightarrow Q$ también se lee "si P, Q"; "Q si P"; "P sólo si Q"; "Q siempre que P"; "suponiendo P, entonces Q";"Q dado que P";"P es suficiente para Q" y "Q es necesario para P".

En el siguiente ejemplo todas las afirmaciones quieren decir lo mismo.

Ejemplo 1.5. a) *Si p es un número par, $p = 2m$ para algún $m \in \mathbb{Z}$.*

b) *$p = 2m$ para algún $m \in \mathbb{Z}$, si p es par.*

c) *p es un número par sólo si $p = 2m$ para algún $m \in \mathbb{Z}$.*

d) *$p = 2m$ para $m \in \mathbb{Z}$ siempre que p sea par.*

e) *Suponiendo que p sea par entonces $p = 2m$ para algún $m \in \mathbb{Z}$.*

f) *p es par es suficiente para que $p = 2m$ para algún $m \in \mathbb{Z}$.*

g) *$p = 2m$ para algún $m \in \mathbb{Z}$ es necesario para que p sea par.*

5. **Bicondicional.** $\leftrightarrow$ **"Si y sólo si"**. La afirmación $P \leftrightarrow Q$ intuitivamente nos dice que es verdadera siempre que P y Q sean ambas verdaderas o ambas falsas, pero que es falsa en caso contrario. De forma más precisa:

P	Q	$P \leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Ejemplo 1.6. *Yo estudiaré Cálculo Diferencial hoy si y sólo si tu lo haces también. Esto se verifica si ambos estudiamos o ambos no lo hacemos, pero claramente si yo lo hago y tu no lo haces no se verifica (o viceversa). Es decir, no puede ser el caso que uno estudie y el otro no.*

Otras formas de leer $P \leftrightarrow Q$, P **si y sólo si** Q, P **si y solamente si** Q, P **es necesario y suficiente para** Q. También podemos escribir a $Q \leftrightarrow P$ en vez de $P \leftrightarrow Q$. Algunas veces abreviamos "si y sólo si" por "sii".

Con estas cinco operaciones básicas $\wedge, \vee, \neg, \rightarrow$ y $\leftrightarrow$ podemos armar afirmaciones más complicadas, como se muestra a continuación.

Ejemplo 1.7. *¿Qué significado tiene $P \vee (Q \rightarrow \neg R)$? Esto lo podemos ver en una tabla de verdad.*

P	Q	R	$\neg R$	$Q \rightarrow \neg R$	$P \vee (Q \rightarrow \neg R)$
V	V	V	F	F	V
V	V	F	V	V	V
V	F	V	F	V	V
V	F	F	V	V	V
F	V	V	F	F	F
F	V	F	V	V	V
F	F	V	F	V	V
F	F	F	V	V	V

Esta tabla la podemos resumir de la siguiente forma.

P	Q	R	$[P$	$\vee$	$(Q$	$\rightarrow$	$\neg R)]$
V	V	V		**V**		F	F
V	V	F		**V**		V	V
V	F	V		**V**		V	F
V	F	F		**V**		V	V
F	V	V		**F**		F	F
F	V	F		**V**		V	V
F	F	V		**V**		V	F
F	F	F		**V**		V	V

En la columna en negrilla queda el valor de verdad de $P \vee (Q \rightarrow \neg R)$. Obsérvese el papel que desempeñan los paréntesis en la afirmación $P \vee (Q \rightarrow \neg R)$. Ellos funcionan como la puntuación en el lenguaje común y elimina ambigüedades.

Ejercicio 1.8. *Hacer la tabla de* $(P \vee Q) \to \neg R$ *y compararla con la tabla de*

$$P \vee (Q \to \neg R).$$

Una **Tautología** es una afirmación que siempre es verdadera, sin importar el valor de verdad de sus componentes.

Ejercicio 1.9. *La afirmación* $P \vee \neg P$ *es una tautología. En efecto observemos su tabla de verdad.*

P	$\neg P$	$P \vee \neg P$
V	F	V
F	V	V

Una **Contradicción** es una afirmación que siempre es falsa sin importar el valor de verdad de sus componentes.

Ejercicio 1.10. *La afirmación* $P \wedge \neg P$ *es una contradicción. Tal como lo vemos en su tabla de verdad.*

P	$\neg P$	$P \wedge \neg P$
V	F	F
F	V	F

Ejercicio 1.11. *La afirmación* $(X \vee Y) \leftrightarrow (\neg X \to Y)$ *es una tautología. En efecto veamos su tabla de verdad*

X	Y	$(X \vee Y)$	$\leftrightarrow$	$(\neg X$	$\to$	$Y)$
V	V	V	**V**	F	V	
V	F	V	**V**	F	V	
F	V	V	**V**	V	V	
F	F	F	**V**	V	F	

1.2. Relaciones entre Afirmaciones.

Las relaciones entre afirmaciones no son propiamente afirmaciones sino algo que llamamos **Meta-afirmaciones**.

Ejemplo 1.12. *Las siguientes frases son Meta-afirmaciones: si la afirmación "Juan es alto y Pedro es bajo" es verdadera, esto implica que la afirmación "Pedro es bajo es verdadera". La afirmación "Juan tiene el cabello negro o Rosa tiene el cabello rojo" es equivalente a la afirmación "Rosa tiene el cabello rojo o Juan tiene el cabello negro".*

Podemos decir entonces que una meta-afirmación es algo que se expresa de algunas afirmaciones. Esta clase de meta-afirmaciones son nuestros prototipos principales. La del primer ejemplo es llamada implicación que es análogo al condicional, y la del segundo ejemplo es llamada equivalencia, análoga al bicondicional y nos ayudarán a construir argumentos válidos.

Implicaciones

Definición 1.13 (Implicación)**.** *Diremos que P implica Q, lo cual denotamos por $P \Rightarrow Q$, si la afirmación $P \to Q$ es una tautología. Es decir, debe ser cierta en cualquier circunstancia, no importando los valores de verdad de las componentes P y Q.*

Obsérvese que el condicional no es lo mismo que la implicación. $P \to Q$ es una afirmación, mientras que $P \Rightarrow Q$ es una meta-afirmación. En realidad $P \Rightarrow Q$ nos dice que no importan los valores de P ó Q para que $P \to Q$ sea verdadera y por eso se puede decir que P siempre implica Q.

A continuación presentamos las implicaciones más importantes que existen, las cuales serán usadas en la construcción de argumentos válidos. Sean P, Q, R y S afirmaciones.

1. $[(P \to Q) \wedge P] \Rightarrow Q$ (Modus Ponens).
2. $[(P \to Q) \wedge \neg Q] \Rightarrow \neg P$ (Modus Tollens).
3. $(P \wedge Q) \Rightarrow P$ (Simplificación).
4. $(P \wedge Q) \Rightarrow Q$ (Simplificación).
5. $Q \Rightarrow (P \vee Q)$ (Adición).
6. $P \Rightarrow (P \vee Q)$ (Adición).
7. $[(P \vee Q) \wedge \neg P] \Rightarrow Q$ (Modus Tollendo Ponens).
8. $[(P \vee Q) \wedge \neg Q] \Rightarrow P$ (Modus Tollendo Ponens).
9. $(P \leftrightarrow Q) \Rightarrow (P \to Q)$ (Bicondicional-Condicional).
10. $(P \leftrightarrow Q) \Rightarrow (Q \to P)$ (Bicondicional-Condicional).
11. $[(P \to Q) \wedge (Q \to P)] \Rightarrow (P \leftrightarrow Q)$ (Condicional-Bicondicional).
12. $[(P \to Q) \wedge (Q \to R)] \Rightarrow (P \to R)$ (Silogismo Hipotetico).
13. $[(P \to Q) \wedge (R \to S) \wedge (P \vee R)] \Rightarrow (Q \vee S)$ (Dilema Constructivo).

Al decir que estas implicaciones son ciertas, lo que estamos diciendo es que los condicionales correspondientes son tautologías. Probemos por ejemplo el "Modus Tollendo Ponens". Para esto debemos ver que $[(P \vee Q) \wedge \neg P] \to Q$ es una tautología y esto lo hacemos por medio de una tabla de verdad.

P	Q	$[(P \vee Q)$	$\wedge$	$\neg P]$	$\rightarrow$	Q
V	V	V	F	F	**V**	
V	F	V	F	F	**V**	
F	V	V	V	V	**V**	
F	F	F	F	V	**V**	

Mirando la columna en negrilla nos damos cuenta que es una tautología. Observamos que en el lenguaje común una afirmación de Modus Tollendo Ponens es muy lógica. Por ejemplo Juan tiene ojos verdes o Rosa el cabello rojo, pero Juan no tiene ojos verdes, luego Rosa tiene el cabello rojo.

Equivalencias.

Definición 1.14. *Diremos que P es equivalente a Q, lo cual denotamos como $P \Leftrightarrow Q$, si la afirmación $P \leftrightarrow Q$ es una tautología. Se puede ver que $P \Leftrightarrow Q$ es verdadero si y sólo si $P \Rightarrow Q$ y $Q \Rightarrow P$ son ambas verdaderas.*

Observe que $P \Leftrightarrow Q$ no es lo mismo que $P \leftrightarrow Q$, pues la primera es una meta-afirmación y la segunda es una afirmación. A continuación presentamos las equivalencias más importantes que existen y también serán usadas en la contrucción de argumentos válidos.

1. $\neg(\neg P) \Leftrightarrow P$ (Doble negación).
2. $(P \vee Q) \Leftrightarrow (Q \vee P)$ (Ley Conmutativa).
3. $(P \wedge Q) \Leftrightarrow (Q \wedge P)$ (Ley Conmutativa).
4. $[(P \vee Q) \vee R] \Leftrightarrow [P \vee (Q \vee R)]$ (Ley Asociativa).
5. $[(P \wedge Q) \wedge R] \Leftrightarrow [P \wedge (Q \wedge R)]$ (Ley Asociativa).
6. $[P \wedge (Q \vee R)] \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)]$ (Ley Distributiva).
7. $[P \vee (Q \wedge R)] \Leftrightarrow [(P \vee Q) \wedge (P \vee R)]$ (Ley Distributiva).
8. $(P \rightarrow Q) \Leftrightarrow (\neg P \vee Q)$ (Definición Alterna del Condicional).
9. $(P \rightarrow Q) \Leftrightarrow (\neg Q \rightarrow \neg P)$ (Contrarrecíproco).
10. $(P \leftrightarrow Q) \Leftrightarrow (Q \leftrightarrow P)$ (Simetría).
11. $(P \leftrightarrow Q) \Leftrightarrow [(P \rightarrow Q) \wedge (Q \rightarrow P)]$ (Bicondicional-Condicional).
12. $[\neg(P \wedge Q)] \Leftrightarrow (\neg P \vee \neg Q)$ (Ley de De Morgan).
13. $[\neg(P \vee Q)] \Leftrightarrow (\neg P \wedge \neg Q)$ (Ley de De Morgan).
14. $[\neg(P \rightarrow Q)] \Leftrightarrow (P \wedge \neg Q)$ (Negación del Condicional).
15. $[\neg(P \leftrightarrow Q)] \Leftrightarrow [(P \wedge \neg Q) \vee (\neg P \wedge Q)]$ (Negación del Bicondicional).

Probemos que $[\neg(P \to Q)] \Leftrightarrow (P \wedge \neg Q)$. En efecto, debemos mostrar que el bicondicional correspondiente es una tautología.

P	Q	$[\neg$	$(P \to Q)]$	$\leftrightarrow$	$(P\wedge$	$\neg Q)$
V	V	F	V	**V**	F	F
V	F	V	F	**V**	V	V
F	V	F	V	**V**	F	F
F	F	F	V	**V**	F	V

Todas estas equivalencias jugarán de ahora en adelante un papel esencial cuando se están haciendo demostraciones. De algunas de ellas se derivan los métodos de demostración que usamos al hacer las pruebas de teoremas. A continuación presentamos algunos ejemplos.

Ejemplo 1.15. *1. $(P \to Q) \Leftrightarrow (\neg Q \to \neg P)$ (Contrarrecíproco). Muchas veces para probar $P \to Q$ resulta más fácil probar su contrarrecíproco $\neg Q \to \neg P$.*

2. $\neg(\neg P) \Leftrightarrow P$ (Doble Negación). El método del absurdo o por contradicción es derivado de la doble negación. Si queremos probar que P es verdadero, suponemos que $\neg P$ es verdadero y si llegamos a una contradicción, se tendría que $\neg(\neg P)$ es verdadero, y como éste es equivalente a P, se concluirá finalmente que P es verdadero.

3. $(P \leftrightarrow Q) \Leftrightarrow [(P \to Q) \wedge (Q \to P)]$ (Bicondicional-Condicional). Nos permitirá concluir que $P \leftrightarrow Q$ es verdadero siempre y cuando ambos condicionales $P \to Q$ y $Q \to P$ lo sean.

4. $(P \to Q) \Leftrightarrow (\neg P \vee Q)$ (Definición alterna del condicional). Es una manera de entender el condicional en términos de la negación y la disyunción. En algunos libros de lógica formal, es así como se define el condicional. Recordemos que dijimos que $P \to Q$ es verdadero si nunca se da el caso en que P sea verdadero y al mismo tiempo Q sea falso. Observemos que la afirmación $\neg P \vee Q$ es verdadera en todos los casos excepto justamente cuando P es verdadero y Q es falso.

5. $[\neg(P \wedge Q)] \Leftrightarrow (\neg P \ \vee \neg Q)$ y $[\neg(P \vee Q)] \Leftrightarrow (\neg P \ \wedge \neg Q)$. Las Leyes de De Morgan las tenemos que tener presentes cuando neguemos disyunciones o conjunciones. Por ejemplo, para negar la afirmación "Yo como y yo bebo" negamos sus dos componentes y cambiamos la conjunción por la disyunción. En otras palabras es "Yo no como o yo no bebo".

Terminología Especial.

(*i*) $\neg Q \to \neg P$ le llamamos el **contrarrecíproco** de $P \to Q$.

(*ii*) $Q \to P$ le llamamos el **recíproco** de $P \to Q$.

Obsérvese que sólo el contrarrecíproco es equivalente a $P \to Q$. Pretender que el recíproco sea equivalente a $P \to Q$ es un grave error y esto es llamado una falacia.

1.3. Argumentos Válidos.

Las pruebas que hemos hecho hasta ahora han sido por medio de tablas de verdad, sin embargo, lo usual en matemáticas es dar afirmaciones que se van encadenando a partir de unas hipótesis hasta llegar a una conclusión deseada. En esta sección miraremos este proceso desde el punto de vista de la lógica, sin embargo a partir del capítulo siguiente haremos pruebas como se hacen en matemáticas, sin tener explícitas las reglas de la lógica, aunque de todas formas reconoceremos que ellas están allí detrás guiándonos en las pruebas.
Argumento: Según la lógica un argumento es una colección de afirmaciones, siendo la última llamada la conclusión y el resto se llaman las premisas.
Argumento Válido: Es aquel argumento cuya conclusión se sigue necesariamente de las premisas. Podríamos decir que un argumento es válido si no podemos asignar valores de verdad a las afirmaciones que lo componen de tal forma que las premisas sean todas verdaderas pero la conclusión sea falsa.

Observemos el siguiente argumento lógico: Si Rosa está bailando o está comiendo, entonces está en su casa. Si Rosa está leyendo entonces no está en su casa. Rosa está bailando. Por tanto Rosa no está leyendo.
Interpretémoslo simbólicamente:
A : Rosa está bailando.
B : Rosa está comiendo.
C : Rosa está en su casa.
D : Rosa está leyendo.

$$\begin{array}{lllll} A & \vee & B & \rightarrow & C \\ D & \rightarrow & \neg C & & \\ A & & & & \\ \hline \neg D & & & & \end{array}$$

Lo anterior es lo mismo que $[(A \vee B \rightarrow C) \wedge (D \rightarrow \neg C) \wedge A] \rightarrow \neg D$. Podríamos hacer una tabla de verdad para probar que es una tautología, pero ésta se hace demasiado larga y tediosa. En vez de seguir usando tablas de verdad, daremos una reglas de inferencia que nos permitirán ir produciendo los encadenamientos necesarios para llegar a la conclusión.

Reglas de Inferencia.

Las reglas de inferencia provienen de las listas de implicaciones y equivalencias vistas anteriormente. Aunque destacaremos sólo las más importantes aclaramos que cualquiera de las implicaciones o equivalencias vistas permiten extraer reglas de inferencia. Ahora las escribiremos en un formato diferente.
Modus Ponens.

$$\begin{array}{lll} P & \rightarrow & Q \\ P & & \\ \hline Q & & \end{array}$$

Modus Tollens.

$$\begin{array}{l} P \quad \rightarrow \quad Q \\ \neg Q \\ \hline \neg P \end{array}$$

Doble Negación.

$$\frac{\neg\ \neg P}{P} \quad \text{y} \quad \frac{P}{\neg\neg P}$$

Repetición.

$$\frac{P}{P}$$

Simplificación.

$$\frac{P \quad \wedge \quad Q}{P} \quad \text{y} \quad \frac{P \quad \wedge \quad Q}{Q}$$

Adjunción. (Note que ésta es nueva, pero obvia)

$$\begin{array}{l} P \\ Q \\ \hline P \quad \wedge \quad Q \end{array}$$

Adición.

$$\frac{P}{P \quad \vee \quad Q} \quad \text{y} \quad \frac{Q}{P \quad \vee \quad Q}$$

Modus Tollendo Ponens.

$$\begin{array}{l} P \quad \vee \quad Q \\ \neg P \\ \hline Q \end{array} \quad \text{y} \quad \begin{array}{l} P \quad \vee \quad Q \\ \neg Q \\ \hline P \end{array}$$

Bicondicional.

$$\frac{P \quad \leftrightarrow \quad Q}{P \quad \rightarrow \quad Q} \quad \text{y} \quad \frac{P \quad \leftrightarrow \quad Q}{Q \quad \rightarrow \quad P}$$

Condicional Bicondicional.

$$\begin{array}{lll} P & \to & Q \\ Q & \to & P \\ \hline P & \leftrightarrow & Q \end{array}$$

Silogismo Hipotético.

$$\begin{array}{lll} P & \to & Q \\ Q & \to & R \\ \hline P & \to & R \end{array}$$

Dilema Constructivo.

$$\begin{array}{lll} P & \to & Q \\ R & \to & S \\ P & \vee & R \\ \hline Q & \vee & S \end{array}$$

Estas reglas de inferencia nos permitirán construir los argumentos válidos. Repetimos, aquí hemos listado sólo las más importantes, pero debemos saber que hay muchas otras reglas de inferencia. Cada implicación dada arriba genera una regla de inferencia y las equivalencias producen dos, de hecho cada vez que se tenga una nueva implicación o una equivalencia se obtienen más reglas de inferencia.

Ejemplo 1.16. *Usemos nuestras reglas para justificar nuestro argumento en el cual concluimos que Rosa no está leyendo. Simbólicamente éste es,*

$$\begin{array}{l} A \vee B \to C \\ D \to \neg C \\ A \\ \hline \neg D \end{array}$$

(1)	$A \vee B \to C$	
(2)	$D \to \neg C$	Las premisas no necesitan justificación
(3)	A	
(4)	$A \vee B$	(3) y Adición.
(5)	C	(1) y (4) Modus Ponens.
(6)	$\neg\neg C$	(5) Doble Negación.
(7)	$\neg D$	(2) y (6) Modus Tollens.

Esta clase de prueba, a menudo llamada una derivación por los lógicos, es una serie de afirmaciones conectadas con meta-afirmaciones que son justamente las justificaciones que estamos escribiendo

en la segunda columna. Nótese que las tres primeras afirmaciones, que son las premisas no las justificamos. Si un argumento tiene una derivación se dice que es derivable. La derivabilidad no depende del valor verdad de las premisas o de la conclusión. Para un argumento puede haber distintas derivaciones.

Ejemplo 1.17. *Veamos otra derivación del argumento anterior. Note que aquí agregamos o adjuntamos $C \to C \Leftrightarrow \neg C \vee C$ la cual es una Tautología, lo cual siempre se puede hacer.*

(1)	$A \vee B \to C$	
(2)	$D \to \neg C$	
(3)	A	
(4)	$A \vee B$	(3) y Adición.
(5)	$\neg(\neg C) \to \neg D$	(2) y Contrarrecíproco.
(6)	$C \to C$	Tautología
(7)	$C \to \neg(\neg C)$	(6) y Doble Negación.
(8)	$C \to \neg D$	(5), (7) y Silogismo Hipotético.
(9)	$A \vee B \to \neg D$	(1) y (8) Silogismo Hipotético.
(10)	$\neg D$	(4) y (9) y Modus Ponens.

Aparentemente estamos hablando de dos cosas diferentes cuando decimos argumento válido y argumento derivable. Sin embargo (aunque no es fácil de probar), tenemos que un argumento es válido si y sólo si es derivable. Así pues, para mostrar que un argumento es válido lo que debemos mostrar es que es derivable, en vez de tratar de hacerlo por medio de tablas de verdad. Para mostrar que un argumento es no válido lo que debemos es tratar de encontrar algunos valores de verdad en las componentes de las afirmaciones de tal manera que todas las premisas resultan verdaderas, pero la conclusión es falsa.

Ejemplo 1.18. *El siguiente argumento es no válido.*

$$\begin{array}{lll} A & \to & R \\ S & \to & H \\ A & \wedge & H \\ \hline R & \wedge & S \end{array}$$

En efecto, si suponemos que A es V; R es V; S es F y H es V obtenemos que $A \to R$ es V; $S \to H$ es V y que $A \wedge H$ también es V, pero $R \wedge S$ es falso. Esto nos permite concluir que el argumento es no válido. Pero debemos tener cuidado, porque con otra escogencia de valores podría ser que todo, premisas y conclusiones, fueran verdaderas. Lo que no quiere decir que el argumento sea válido.

En un argumento debemos tener cuidado para que las premisas no sean contradictorias entre sí, ya que de algo falso se puede inferir cualquier cosa. Cuando se tienen premisas contradictorias se dice que son inconsistentes. Por el contrario, premisas consistentes son las que no son contradictorias. Nótese que se pueden producir argumentos válidos a partir de premisas inconsistentes, sin embargo, estos no son útiles, ya que de una contradicción es posible derivar cualquier cosa. Por ejemplo los

argumentos:

$$\begin{array}{l} \neg J \vee S \\ \neg L \rightarrow \neg S \\ J \wedge \neg L \\ \hline G \end{array} \quad \text{y} \quad \begin{array}{l} \neg J \vee S \\ \neg L \rightarrow \neg S \\ J \wedge \neg L \\ \hline \neg G \end{array}$$

Son ambos argumentos válidos. En efecto veamos derivaciones para ellos.

(1)	$\neg J \vee S$	
(2)	$\neg L \rightarrow \neg S$	
(3)	$J \wedge \neg L$	
(4)	J	(3) y Simplificación.
(5)	$\neg L$	(3) y Simplificación.
(6)	$\neg S$	(2) y (5) Modus Ponens.
(7)	$J \vee G$	(4) adición.
(8)	$\neg J$	(6) y (1) Modus Tollendo Ponens.
(9)	G	(7) y 8) Modus Tollendo Ponens.

(1)	$\neg J \vee S$	
(2)	$\neg L \rightarrow \neg S$	
(3)	$J \wedge \neg L$	
(4)	J	(3) y Simplificación.
(5)	$\neg L$	(3) y Simplificación.
(6)	$\neg S$	(2) y (5) Modus Ponens.
(7)	$J \vee \neg G$	(4) Adición.
(8)	$\neg J$	(6) y (1) Modus Tollendo Ponens.
(9)	$\neg G$	(7) y 8) Modus Tollendo Ponens.

Recordemos que un argumento válido es aquel que admite una derivación. Una cosa es que las premisas sean contradictorias y otra cosa es que exista un derivación, o lista de afirmaciones justificada por la regla de inferencia. En los dos ejemplos anteriores si unimos las premisas con conjunciones así: $[(\neg J \vee S) \wedge (\neg L \rightarrow \neg S) \wedge (J \wedge \neg L)]$ y hacemos la tabla de verdad de esta afirmación encontraríamos que la afirmación es una contradicción, de la cual podríamos concluir cualquier cosa que deseemos.

Hagamos algunos ejemplos para detallar un poco más el proceso de probar que un argumento es válido.

Ejemplo 1.19. *Muestre que el siguiente argumento es válido.*

$$\begin{array}{l} P \longrightarrow Q \\ R \longrightarrow S \\ \hline (P \vee R) \longrightarrow (Q \vee S) \end{array}$$

Solución: *En este caso se tiene que*

(1)	$P \longrightarrow Q$	
(2)	$R \longrightarrow S$	
(3)	$\neg P \vee Q$	*(1) y Definición Alterna del Condicional*
(4)	$\neg R \vee S$	*(2) y Definición Alterna del Condicional*
(5)	$(\neg P \vee Q) \vee S$	*(3) y Adición*
(6)	$(\neg R \vee S) \vee Q$	*(4) y Adición*
(7)	$\neg P \vee (Q \vee S)$	*(5) y Asociativa del* $\vee$
(8)	$\neg R \vee (Q \vee S)$	*(6), Asociativa y Conmutativa del* $\vee$
(9)	$[\neg P \vee (Q \vee S)] \wedge [\neg R \vee (Q \vee S)]$	*(7), (8) y Adjunción*
(10)	$(\neg P \wedge \neg R) \vee (Q \vee S)$	*(9) y Distributiva del* $\vee$ *con respecto al* $\wedge$
(11)	$[\neg(P \vee R)] \vee (Q \vee S)$	*(10) y Ley de De Morgan*
(12)	$(P \vee R) \longrightarrow (Q \vee S)$	*(11) y Definición Alterna del Condicional*

En realidad en este caso lo que se hizo fue desglosar la tesis $(P \vee R) \longrightarrow (Q \vee S)$, lo que es equivalente a $\neg(P \vee R) \vee (Q \vee S)$ y si seguimos este proceso nos damos cuenta que necesitamos que $\neg P \vee (Q \vee S)$ y $\neg R \vee (Q \vee S)$ sean válidos, lo cual podemos obtener de la hipótesis usando adición. Este tipo de racionamiento, "a la inversa", es muy común para esta clase de problemas.

Ejemplo 1.20. *Muestre que el siguiente argumento es válido.*

$$\begin{array}{l} P \longrightarrow \neg Q \\ \neg P \longrightarrow \neg R \\ R \ \vee \neg S \\ \hline \neg(Q \wedge S) \end{array}$$

Solución: *En este caso tenemos lo siguiente*

(1)	$P \longrightarrow \neg Q$	
(2)	$\neg P \longrightarrow \neg R$	
(3)	$R \ \vee \neg S$	
(4)	$R \longrightarrow P$	*(2) y Contrarecíproco*
(5)	$R \longrightarrow \ \neg Q$	*(1), (4) y Silogismo Hipotético*
(6)	$S \ \vee \neg S$	*Tautología*
(7)	$\neg S \longrightarrow \ \neg S$	*(6) y Definición Alterna del Condicional*
(8)	$(R \ \vee \neg S) \longrightarrow (\neg Q \ \vee \neg S)$	*(5), (7) y Ejercicio 1.19*
(9)	$\neg Q \ \vee \neg S$	*(3), (8) y Modus Ponens*
(10)	$\neg(Q \wedge S)$	*(9) y Ley de De Morgan*

Cabe resaltar que siempre podemos agregar Tautologías a nuestros argumentos, tal como lo hicimos en este ejercicio.

1.4. Cuantificadores.

A veces encontramos expresiones que involucran una o varias variables, tales como $8 \leq x^3$; $y^2 = 3$ ó $x + y^2 = 7$, de las cuales no podemos decir que sean expresiones verdaderas o falsas, a menos que digamos algo sobre las variables. Mientras no se haya especificado como son las variables, dichas variables se llaman libres. Una expresión con variables libres no es una afirmación.

Retomemos $8 \leq x^3$, preguntémonos ¿Cuándo sería cierta dicha afirmación? La respuesta sería: "para todo número real $2 \leq x$" , así que la expresión "para todo número real $2 \leq x$, se tiene $8 \leq x^3$" sí es una afirmación, allí la variable no es libre, pues hemos puesto condiciones para ella. En este caso decimos que la variable está amarrada, acotada o delimitada. Esta variable la hemos amarrado por medio de la expresión "para todo número real $2 \leq x$". Esta expresión es un ejemplo de un cuantificador. También podríamos haber dicho, "para todo número real $x < 1$, se tiene $8 \leq x^3$", pero esta última afirmación es falsa. Podemos decir que x está delimitada por el cuantificador "para todo número real $x < 1$". En otras palabras cuando tengamos expresiones donde aparezcan variables libres, las podemos convertir en afirmaciones "amarrando" sus variables por medio de cuantificadores. Debemos ser muy cuidadosos en el manejo de los cuantificadores, pues es muy fácil introducir errores si ellos no se manejan bien. Muchas veces es recomendable usar los símbolos matemáticos de ellos para poder usarlos mejor.

El lenguaje corriente es muy impreciso en el uso de los cuantificadores, sin embargo en el lenguaje matemático no debe haber duda con su manejo. La frase "Alguien es golpeado por un carro cada hora" ¿Qué significa? Que una misma persona es golpeada por un carro cada hora. Claro que no, lo que queremos decir es que para cada hora existe una persona que es golpeada por un carro. La segunda frase es más precisa que la primera. ¿Por qué lo es? Veremos que ella se adecúa más al lenguaje matemático, cuando hay dos cuantificadores. Por eso, cuando veamos que hay afirmaciones que involucran uno o varios cuantificadores, es conveniente reescribir simbólicamente para que los cuantificadores se vean explícitamente y los podamos manejar correctamente.

Cuantificador Universal.

Definición 1.21. *Sean $P(x)$ una expresión donde x aparece libre y U una colección de los posibles valores de x. Un cuantificador universal aplicado a $P(x)$ produce una afirmación denotada por*

$$(\forall x \text{ en } U)P(x),$$

la cual es verdadera si $P(x)$ es válida para todos los posibles valores de x en U y será falsa en cualquier otro caso.

Ejemplo 1.22. *La afirmación*

$$(\forall x \text{ en } [2, +\infty))(x^2 - 4 \geq 0)$$

es verdadera, pues si x está en $[2, +\infty)$, entonces $x \geq 2$, luego $x^2 \geq 4$ y por tanto $x^2 - 4 \geq 0$ (note que x fue tomado arbitrariamente en $[2, +\infty)$). Por otro lado, la afirmación $(\forall x \text{ en } \mathbb{R})(x^2 - 4 \geq 0)$ es falsa, porque no todos los valores de x en $\mathbb{R}$ hacen que $x^2 - 4$ sea mayor o igual que cero. Por ejemplo si $x = 1$ se tiene que $x^2 - 4 = 1 - 4 = -3$, el cual es menor que cero.

Si la colección U se sobreentiende por el contexto, entonces escribimos siplemente $(\forall x)P(x)$. La afirmación $(\forall x$ en $U)P(x)$ se puede leer de cualquiera de las siguientes formas: para todos los valores de x en U, la afirmación $P(x)$ es verdadera; la afirmación $P(x)$ es verdadera para todo x en U; todos los valores de x en U satisfacen $P(x)$; para todo x en U se tiene $P(x)$; para todo x en U, $P(x)$.

Ejemplo 1.23. *Sea $P(x)$ la afirmación "el perro x es café". Sea D la colección de todos los perros del mundo. $(\forall x$ en $D)P(x)$ quiere decir "Todo perro en el mundo es café", la cual indudablemente es falsa. Obsérvese que cuando se amarra la variable ya no la necesitamos explicitar, esto también quiere decir que el nombre de la variable es intrascendente. Así pues, las afirmaciones $(\forall x$ en $D)P(x)$ y $(\forall z$ en $D)P(z)$ tienen el mismo significado.*

Cuantificador Existencial.

Definición 1.24. *Sean $P(x)$ una expresión donde x aparece libre y U una colección de los posibles valores de x. Un cuantificador existencial aplicado a $P(x)$ produce una afirmación denotada por*

$$(\exists x \ \ en \ \ U)P(x),$$

la cual es verdadera si $P(x)$ es válida al menos para algún valor de x en la colección U. Si esto no se cumple, entonces es falsa.

Ejemplo 1.25. *Decir que la afirmación "Existe un estudiante en esta clase de cabello negro" es verdadera, significa que hay uno, dos, tres o más estudiantes que tienen cabello negro. Inclusive todos podrían tener el cabello negro.*

En particular si $(\forall x$ en $U)P(x)$ es verdadero, entonces $(\exists x$ en $U)P(x)$ también lo es. La afirmación $(\exists x$ en $U)P(x)$ se puede leer de cualquiera de las siguientes formas: existe un x en U tal que $P(x)$ se satisface; para algún valor de x, tenemos que $P(x)$ es cierto; existe algún x en U tal que $P(x)$ es verdadero; existe al menos un valor x en U tal que $P(x)$ se satisface.

Ejemplo 1.26. *Si $P(x)$ es la afirmación: "El perro es café". D es la colección de todos los perros del mundo, entonces $(\exists x$ en $D)P(x)$ es claramente verdadera.*

Ejemplo 1.27. *La afirmación $(\exists x$ en $\mathbb{Z})(x^3+1=0)$ es verdadera. Para demostrarlo solo debemos hallar un elemento de $\mathbb{Z}$ que satisfaga la propiedad, por ejemplo tome $x=-1$ (de hecho es el único) el cual está en $\mathbb{Z}$ y note además que $x^3+1=(-1)^3+1=-1+1=0$.*

Obsérvese que la implicación $(\forall x)P(x) \Rightarrow (\exists x)P(x)$ es cierta; pero no al revés, este hecho será explicado un poco mejor más adelante.

Cuantificadores con varias variables.

Si en una expresión aparece más de una variable libre, podemos usar más de un cuantificador.

Ejemplo 1.28. *En la expresión $y = x^2 + 2x$ hay dos variables libres. Ahora si consideramos $(\forall x$ en $\mathbb{R})(\exists y$ en $\mathbb{R})(y-x^2+2x=0)$ es un afirmación verdadera, pues para cualquier x que yo tome (real) puedo encontrar un y que satisface la ecuación (considere $y=x^2-2x$). Sin embargo, dicha afirmación no es lo mismo que $(\exists y$ en $\mathbb{R})(\forall x$ en $\mathbb{R})(y-x^2+2x=0)$, la cual que dice que existe un y que satisafce $x^2-2x=y$ para todo x que yo tome en los reales, claramente la afirmación es falsa, pues y depende de x, de la siguiente forma $y=y(x)=x^2-2x$.*

Por tanto el orden de los cuantificadores sí importa y es un error muy común cambiar su orden, aunque algunas veces, como veremos enseguida, sí los podemos cambiar de posición.

Ejemplo 1.29. *Volvamos al ejemplo "Alguien es golpeado por un carro cada hora". Escribámoslo simbólicamente y correctamente según el sentido que le queramos dar. Tenemos dos variables. Los posibles valores de x son todas las personas posibles y los posibles valores de t son todas las horas. $C(x,t)$: Persona x es golpeada por un carro en la hora t. Entonces la expresión de arriba la escribimos $(\forall t)(\exists x)C(x,t)$ y no por $(\exists x)(\forall t)C(x,t)$, que siginifica que existe una persona que es golpeada por un carrro todo el tiempo. Si queremos más precisión debería tomar 3 variables. $P(x,c,t)$: Persona x golpeada por el carro c a las t horas. Los posibles valores de x son todas las personas, los posibles valores de t son todos las horas y los posibles valores de c son todos los carros. Y la expresión nos quedará $(\forall t)(\exists x)(\exists c)P(x,c,t)$ la cual es diferente de $(\exists x)(\exists c)(\forall t)P(x,c,t)$, que significa que existe una persona y un carro, tal que esa persona es golpeada por ese carro todo el tiempo.*

Cuando hay dos cuantificadores aparecen ocho combinaciones. Algunas Combinaciones son equivalentes pero otras no. Lo vemos en los cuadros siguientes. Sea $P(x,y)$ una expresión con dos variables libres.

$$\begin{array}{ccc} (\forall x)(\forall y)P(x,y) & \Leftrightarrow & (\forall y)(\forall x)P(x,y) \\ \Downarrow & & \Downarrow \\ (\exists x)(\forall y)P(x,y) & & (\exists y)(\forall x)P(x,y) \end{array}$$

$$\begin{array}{ccc} (\forall x)(\forall y)P(x,y) & \Leftrightarrow & (\forall y)(\forall x)P(x,y) \\ \Downarrow & & \Downarrow \\ (\forall x)(\exists y)P(x,y) & & (\forall y)(\exists x)P(x,y) \end{array}$$

$$\begin{array}{ccc} (\forall x)(\exists y)P(x,y) & & (\forall y)(\exists x)P(x,y) \\ \Downarrow & & \Downarrow \\ (\exists x)(\exists y)P(x,y) & \Leftrightarrow & (\exists y)(\exists x)P(x,y) \end{array}$$

Nótese que si hubiera más variables habría muchos más casos.

Negando afirmaciones con Cuantificadores.

Ejemplo 1.30. *Neguemos: "Todo alumno en este salón tiene cabello negro". Para ello basta decir "Existe un alumno en este salón que no tiene el cabello negro".*

Más exactamente, tenemos lo siguiente

$$\neg(\forall x)P(x) \Leftrightarrow (\exists x)(\neg P(x)).$$

Esto quiere decir que para negar una afirmación que contiene un para todo, simplemente, convertimos el cuantificador universal en un existencial y negamos lo que se exprese de la variable. Obsérvese que en el ejemplo anterior no es necesario decir que todo alumno en este salón no tiene el cabello negro,

que simbólicamente sería $(\forall x)(\neg P(x))$. Es decir $(\forall x)(\neg P(x))$ no es lo mismo que $(\exists x)(\neg P(x))$. Similarmente, negar que "Existe un alumno con cabello morado" es equivalente a decir que "Todos los alumnos no tienen el cabello morado".
Más exactamente,

$$\neg(\exists x)P(x) \Leftrightarrow (\forall x)(\neg P(x)).$$

Así que para negar una afirmación que contiene un existencial simplemente convertimos el cuantificador existencial en un universal y negamos lo que se exprese de la variable. Y no estaría bien negado decir que "Existe un alumno que no tiene el cabello morado".

Negando afirmaciones con más de un Cuantificador.
Neguemos la afirmación $[(\forall x)(\exists y)P(x,y)]$. Hagámoslo por pasos:

$$\neg[(\forall x)(\exists y)P(x,y) \Leftrightarrow (\exists x)(\neg(\exists y)P(x,y)) \Leftrightarrow (\exists x)(\forall y)(\neg P(x,y)).$$

Por tanto, para negar afirmaciones que involucran varios cuantificadores, estos se cambian entre sí, sin cambiar las variables y la expresión final se niega, como en el siguiente ejemplo.

$$\neg[(\forall y)(\exists w)(\forall x)(\forall m)[y+w^2-x=m]] \Leftrightarrow (\exists y)(\forall w)(\exists x)(\exists m)[y+w^2-x\neq m].$$

Por esto es muy importante la simbolización, pues el trabajo de los cuantificadores en forma simbólica se hace más fácil. Sin embargo con bastante práctica se podrá trabajar con ellos en forma implícita.

Ejemplo 1.31. *Negemos lo siguiente:* $(\forall x \text{ en } U)(\exists y \text{ en } V)(\forall z \text{ en } W)\{P(x) \rightarrow [Q(y) \vee R(z)]\}$. *Siguiendo las ideas antes expresadas, la negación nos quedaría de la siguiente forma*

$$(\exists x \text{ en } U)(\forall y \text{ en } V)(\exists z \text{ en } W)\{\neg\{P(x) \rightarrow [Q(y) \vee R(z)]\}\}.$$

Note que tenemos que negar un condicional, es decir debemos usar $\neg(A \rightarrow B) \Leftrightarrow (A \wedge \neg B)$. *Así que la negación seguiría de la siguiente forma*

$$(\exists x \text{ en } U)(\forall y \text{ en } V)(\exists z \text{ en } W)\{P(x) \wedge \neg[Q(y) \vee R(z)]\}\}.$$

Finalmente usando la ley de De Morgan llegamos al resultado

$$(\exists x \text{ en } U)(\forall y \text{ en } V)(\exists z \text{ en } W)\{P(x) \wedge [\neg Q(y) \wedge \neg R(z)]\}\}.$$

Reglas de Inferencia que Involucran Cuantificadores.

1. **(Ejemplificación Universal)** Para a un elemento arbitrario en U,

$$\frac{(\forall x \text{ en } U)P(x)}{P(a)}$$

2. **(Ejemplificación Existencial)** Siendo b algún elemento de U y sin tener b ningún otro significado en el argumento dado,

$$\frac{(\exists x \text{ en } U)P(x)}{P(b)}$$

3. **(Generalización Universal)**. Para c un elemento arbitrario en U,

$$\frac{P(c)}{(\forall x \text{ en } U)P(x)}$$

4. **(Generalización Existencial)** Para d un elemento de U,

$$\frac{P(d)}{(\exists x \text{ en } U)P(x)}$$

Ejemplo 1.32. *Consideremos el siguiente argumento: Todo perro que es inteligente y ágil le gusta brincar. Todo Dálmata es ágil. Hay un Dálmata que no le gusta brincar. Entonces hay un perro que no es inteligente.*

Con el fin de entender, por qué se deduce lógicamente que hay un perro que no es inteligente, reescribamos el argumento en forma simbólica y hagamos una derivación para dicha conclusión. Sea U la colección de los perros, $I(x)$: el perro x es inteligente, $A(x)$: el perro x es ágil, $B(x)$: el perro x le gusta brincar, $D(x)$: el perro x es Dálmata. El argumento queda traducido de la siguiente manera.

(1)	$(\forall x \text{ en } U)\{[I(x) \wedge A(x)] \rightarrow B(x)\}$	
(2)	$(\forall x \text{ en } U)(D(x) \rightarrow A(x))$	
(3)	$(\exists x \text{ en } U)(D(x) \wedge \neg B(x))$	
		Debemos concluir $(\exists x \text{ en } U)(\neg I(x))$.
(4)	$D(a) \wedge \neg B(a)$	(3) y Ejemplificación Existencial.
(5)	$D(a) \rightarrow A(a)$	(2) y Ejemplificación Universal.
(6)	$D(a)$	(4) Simplificación.
(7)	$A(a)$	(5) y (6) Modus Ponens.
(8)	$[I(a) \wedge A(a)] \rightarrow B(a)$	(1) y Ejemplificación Universal.
(9)	$\neg B(a)$	(4) y Simplificación.
(10)	$\neg(I(a) \wedge A(a))$	(8) y (9) Modus Tollens.
(11)	$\neg I(a) \vee \neg A(a)$	(10) y De morgan.
(12)	$\neg[\neg A(a)]$	(7) y Doble Negación.
(13)	$\neg I(a)$	(11), (12) y Modus Tollendo Ponens.
(14)	$(\exists x \text{ en } U)(\neg I(x))$	(13) y Generalización Existencial

Obsérvese el uso de la letra a en (4), antes de esta línea no estaba siendo usada. En (5) y en (8) no hay problema de retomar la misma letra a pues se está usando Ejemplificación Universal. Obsérvese que de $\neg(I(a))$ no podemos concluir por Generalización Universal que $(\forall x \text{ en } U)(\neg I(x))$ pues en ese caso a no es arbitrario en U, ya que la primera vez que lo utilizamos apareció de una Ejemplificación Existencial. Veamos otro ejemplo.

Ejemplo 1.33. *Escribir una derivación para*

(1)	$(\forall a \text{ en } V)(N(a) \to B(a))$	
(2)	$(\exists b \text{ en } V)(N(b) \wedge D(b))$	
		Probar $(\exists c \text{ en } V)[B(c) \wedge D(c)]$
(3)	$N(d) \wedge D(d)$	(2) y Ejemplificación Existencial.
(4)	$N(d) \to B(d)$	(1) y Ejemplificación Universal
(5)	$N(d)$	(3) y Simplificación.
(6)	$D(d)$	(3) y Simplificación.
(7)	$B(d)$	(4), (5) y Modus Ponens
(8)	$B(d) \wedge D(d)$	(5), (6) y Adjunción.
(9)	$(\exists c \text{ en } V)(B(c) \wedge D(c))$	(8) y Generalización Existencial.

Note que el nombre de las variables en (1), (2) y (9) no es importante, todas las podríamos llamar x.

Ejemplo 1.34.

(1)	$(\forall x \text{ en } W)(\exists y \text{ en } W)\{E(x) \to [M(x) \vee N(y)]\}$	
(2)	$\neg(\forall x \text{ en } W)[M(x)]$	
(3)	$(\forall x \text{ en } W)[E(x)]$	
		Probar $(\exists x \text{ en } W)[N(x)]$
(4)	$(\exists x \text{ en } W)(\neg M(x))$	(2) y Negación Universal.
(5)	$\neg M(a)$	(4) y Ejemplificación Existencial.
(6)	$E(a)$	(3) y Ejemplificación Universal.
(7)	$(\exists y \text{ en } W)\{E(a) \to [M(a) \vee N(y)]\}$	(1) y Ejemplificación Universal.
(8)	$E(a) \to M(a) \vee N(b)$	(7) y Ejemplificación Existencial.
(9)	$M(a) \vee N(b)$	(6), (8) y Modus Ponens.
(10)	$N(b)$	(5), (9) y Modus Tollendo Ponens.
(11)	$(\exists x \text{ en } W)(N(x))$	(10) y Generalización Existencial.

Hay que estar alertas en este tipo de ejercicios, pues puede haber un conjunto de premisas inconsistente, como se ilustra en el siguiente ejemplo.

Ejemplo 1.35. *Toda cucaracha que es inteligente come basura. Hay una cucaracha que le gusta el mugre pero no el polvo. Para toda cucaracha, no es el caso de que le guste el mugre o coma basura. Entonces existe una cucaracha para la cual no es el caso que si no es inteligente entonces le gusta el polvo.*

Sea C la colección de cucarachas, $I(x)$: la cucaracha x es inteligente, $B(x)$: la cucaracha x come basura, $M(x)$: la cucaracha x le gusta el mugre, $P(x)$: la cucaracha x le gusta el polvo.

(1)	$(\forall x \text{ en } C)(I(x) \to B(x))$	
(2)	$(\exists x \text{ en } C)(M(x) \wedge \neg P(x))$	
(3)	$(\forall x \text{ en } C)(\neg(M(x) \vee B(x)))$	
		Probar $(\exists x \text{ en } C)(\neg(\neg I(x) \to P(x)))$
(4)	$M(c) \wedge \neg P(c)$	(2) y Ejemplificación Existencial.
(5)	$\neg(M(c) \vee B(c))$	(3) y Ejemplificación Universal.
(6)	$I(c) \to B(c)$	(1) y Ejemplificación Universal.
(7)	$M(c)$	(4) y Simplificación.
(8)	$\neg P(c)$	(4) y Simplificación.
(9)	$\neg M(c) \wedge \neg B(c)$	(5) y De Morgan.
(10)	$\neg M(c)$	(9) y Simplificación.
(11)	$M(c) \vee (\neg(\neg(I(c)) \to P(c)))$	(7) y Adición.
(12)	$\neg(\neg I(c) \to P(c))$	(10),(11) y Modus Tollendo Ponens.
(13)	$(\exists x \text{ en } C)(\neg(\neg I(x) \to P(x)))$	(12) y Generalización Existencial.

En este ejercicio observamos que el conjunto de premisas es inconsistente, ya que de ellas, se deduce tanto $M(c)$ como $\neg M(c)$. Sin embargo, la derivación existe y el argumento es válido.

1.5. Ejercicios

1. ¿Cuáles de las siguientes expresiones son afirmaciones?

 a) París es la capital de Francia.

 b) Cállese.

 c) ¿Será que llueve el Lunes?

 d) Llámame el jueves si estás en la cuidad.

2. Suponga que A es un enunciado verdadero, B es un enunciado falso, C es un enunciado falso y D es un enunciado verdadero. ¿Cuáles de las siguientes afirmaciones son ciertas y cuáles son falsas?

 a) $(A \vee C) \to D$.

 b) $(C \wedge D) \to B$.

 c) $(A \wedge B) \to \neg C$.

 d) $[\neg D \ \vee \neg C] \leftrightarrow (\neg B)$.

 e) $(D \wedge A) \to (B \wedge C)$.

 f) $C \to [D \vee (A \wedge B)]$

 g) $(A \to \neg D) \vee (A \to \neg B)$

 h) $[\neg A \to (\neg D \vee A)] \to B$

3. Haga una tabla de verdad para cada una de las siguientes afirmaciones.

 a) $(P \ \wedge \neg Q) \to R$.

 b) $(R \to S) \ \wedge \ \neg R$.

 c) $X \vee (\neg Y \vee Z)$.

 d) $(A \vee B) \wedge (A \vee C)$.

 e) $(P \wedge R) \vee \ \neg(Q \wedge S)$.

 f) $X \ \to \ \neg Y$.

g) $(R \to S) \leftrightarrow R$.

h) $\neg M \to (N \wedge L)$.

i) $(E \leftrightarrow F) \leftrightarrow (E \leftrightarrow G)$

j) $(P \to R) \ \vee \neg(Q \leftrightarrow S)$

4. ¿Cuáles de las siguientes afirmaciones son una tautología, contradicción o ninguna de las dos?

 a) $P \vee (\neg P \wedge Q)$.

 b) $(X \vee Y) \leftrightarrow (\neg X \to Y)$.

 c) $(A \ \wedge \ \neg B) \wedge (\neg A \vee B)$.

 d) $[Z \vee (\neg Z \vee W)] \wedge \neg(W \wedge U)$.

 e) $[L \to (M \to N)] \to [M \to (L \to N)]$.

 f) $[(X \leftrightarrow Z) \wedge (X \leftrightarrow Y)] \wedge X$.

 g) $[(P \leftrightarrow \ \neg Q) \wedge P] \wedge Q$.

5. Sean P un enunciado, TA una tautología y sea CO una contradicción.

 a) Muestre que $P \vee TA$ es una tautología.

 b) Pruebe que $T \wedge CO$ es una contradicción.

 c) Muestre que $P \wedge TA \Leftrightarrow P$.

 d) Pruebe que $P \vee CO \Leftrightarrow P$.

6. Sean P, Q, R y S afirmaciones. Pruebe que las siguientes implicaciones son verdaderas.

 a) $\neg(P \to Q) \Rightarrow P$.

 b) $[(P \to Q) \wedge (P \to \ \neg Q)] \Rightarrow \neg P$.

 c) $(P \to Q) \Rightarrow [(P \wedge R) \to (Q \wedge R)]$.

 d) $[P \wedge (Q \leftrightarrow R)] \Rightarrow [(P \wedge R) \leftrightarrow R]$.

 e) $[P \to (Q \wedge R)] \Rightarrow [(P \wedge Q) \leftrightarrow (P \wedge R)]$.

 f) $[(P \leftrightarrow R) \wedge (Q \leftrightarrow S)] \Rightarrow [(P \vee Q) \leftrightarrow (R \vee S)]$.

7. Sean P, Q, A y B afirmaciones. Pruebe que las siguientes equivalencias son verdaderas.

 a) $(P \wedge P) \Leftrightarrow P$

 b) $(P \vee P) \Leftrightarrow P$

 c) $P \Leftrightarrow [P \vee (P \wedge Q)]$.

 d) $P \Leftrightarrow [P \wedge (P \vee Q)]$.

 e) $(P \leftrightarrow Q) \Leftrightarrow [(P \to Q) \wedge (\neg P \to \ \neg Q)]$.

 f) $[P \to (A \wedge B)] \Leftrightarrow [(P \to A) \wedge (P \to B)]$.

 g) $[P \to (A \vee B)] \Leftrightarrow [(P \ \wedge \ \neg A) \to B]$.

 h) $[(A \vee B) \to Q] \Leftrightarrow [(A \to Q) \wedge (B \to Q)]$.

 i) $[(A \wedge B) \to Q] \Leftrightarrow [(A \to Q) \vee (B \to Q)]$.

 j) $[(A \wedge B) \to Q] \Leftrightarrow [A \to (B \to Q)]$.

8. Niegue cada una de las siguientes afirmaciones.

 a) $3 < 5$ o $7 \geq 8$.

 b) Existe $M > 0$, tal que para todo $x \in A$, se tiene $|f(x)| \leq M$.

 c) Para todo $x > 0$, se tiene que $|f(x)| > 1$ o $|g(x)| < 2$.

 d) Si $y = 3$, entonces $y^2 = 7$.

 e) Si $f(x) = 0$, entonces $x \in A$ o $x \in B$.

 f) $a - b = c$ sii $a = b + c$.

 g) Para todo $\epsilon > 0$, existe $\delta > 0$ tal que si $|x - x_0| < \delta$, entonces $|f(x) - L| < \epsilon$.

 h) $(\forall\, x > 0)(\exists\, y > 0)\{\neg P(x) \leftrightarrow [P(y) \wedge R(x)]\}$.

 i) $(\forall\, \epsilon > 0)(\exists\, \delta > 0)\{|x - 1| < \delta \rightarrow |f(x) - f(1)| < \epsilon\}$.

 j) $(\forall\, R > 0)(\exists\, x, y \text{ en } A)\{[|x - y| < R \ \wedge\ x^2 \neq y^2] \rightarrow |x^2 + y| \geq 2\}$.

9. Simplifique las siguientes afirmaciones.

 a) $\neg(P \rightarrow \neg Q)$.

 b) $A \rightarrow (A \wedge B)$.

 c) $(X \wedge Y) \rightarrow X$.

 d) $\neg(M \vee L) \wedge L$.

 e) $(P \rightarrow Q) \vee Q$.

 f) $\neg(X \rightarrow Y) \vee Y$.

10. Por cada uno de los siguientes argumentos, si es válido, dé una derivación, y si no es válido justifique.

 a) Si la comida es verde, entonces está cruda. Si la comida hiede entonces está rancia. La comida es verde o está rancia. Luego la comida está cruda o hiede.

 b) Si a Susan le gusta el pescado, entonces le gustan las cebollas. Si a Susan no le gusta el ajo entonces no le gustan las cebollas. Si le gusta el ajo, entonces le gustan las guayabas. Le gusta el pescado o le gusta el cilantro. No le gustan las guayabas. Por tanto a Susan le gusta el cilantro.

 c) No es el caso que Fred toque tanto guitarra como flauta. Si Fred no toca guitarra y no toca flauta, entonces él toca órgano y arpa. Si él toca arpa, entonces toca órgano. Luego Fred toca órgano.

 d) Si tu robas un banco, vas a la cárcel. Si vas a la cárcel, tu no te diviertes. Si tienes vacaciones, tu te diviertes. Tu robas un banco o tienes vacaciones. Por tanto tu vas a la cárcel o te diviertes.

11. Por cada uno de los siguientes argumentos, si es válido, dé una derivación, y si no es válido justifique.

 a)
 $$\frac{\begin{array}{l} P \longrightarrow Q \\ R \longrightarrow S \end{array}}{(P \wedge R) \longrightarrow (Q \wedge S)}$$

 b)
 $$\frac{P \longrightarrow Q}{(P \vee R) \longrightarrow (Q \vee R)}$$

c)
$$\begin{array}{l} P \wedge Q \\ (P \vee Q) \to R \\ \hline R \end{array}$$

d)
$$\begin{array}{l} E \to F \\ \neg G \to \neg F \\ H \to I \\ E \vee H \\ \hline G \vee I \end{array}$$

e)
$$\begin{array}{l} P \to Q \\ \neg R \to (S \to T) \\ R \vee (P \vee T) \\ \hline Q \vee S \end{array}$$

f)
$$\begin{array}{l} \neg X \to Y \\ \neg X \to Z \\ \hline \neg Z \to \neg Y \end{array}$$

g)
$$\begin{array}{l} L \to M \\ (M \vee N) \to (L \to K) \\ \neg P \wedge L \\ \hline K \end{array}$$

h)
$$\begin{array}{l} \neg A \to (B \to \neg C) \\ C \to \neg A \\ (\neg D \vee A) \to \neg\neg C \\ \neg D \\ \hline \neg B \end{array}$$

i)
$$\begin{array}{l} (A \longrightarrow C) \vee B \\ \neg B \longrightarrow \neg D \\ (D \longrightarrow S) \longrightarrow (C \longrightarrow D) \\ S \wedge A \\ \hline A \longrightarrow B \end{array}$$

j)
$$\begin{array}{l} \neg B \longrightarrow \neg C \\ \neg B \longrightarrow \neg D \\ (A \wedge B) \longrightarrow C \\ C \longrightarrow \neg B \\ C \vee D \\ \hline A \longrightarrow \neg B \end{array}$$

k)
$$\begin{array}{l} (C \wedge B) \longrightarrow D \\ \neg D \\ C \vee D \\ \hline B \longrightarrow A \end{array}$$

l)
$$\begin{array}{l} \neg D \longrightarrow \neg (C \wedge B) \\ D \longrightarrow A \\ \neg A \\ C \vee D \\ \hline B \longrightarrow A \end{array}$$

m)
$$\begin{array}{l} A \longrightarrow C \\ C \vee D \\ C \longrightarrow B \\ B \longrightarrow \neg C \\ B \longrightarrow \neg D \\ \hline \neg A \end{array}$$

n)
$$\begin{array}{l} E \longrightarrow (B \longrightarrow D) \\ (C \longrightarrow D) \longrightarrow B \\ A \vee D \\ A \longrightarrow D \\ \hline E \longrightarrow D \end{array}$$

ñ)
$$\begin{array}{l} (P \longrightarrow Q) \longrightarrow \neg R \\ S \longrightarrow (R \vee T) \\ T \longrightarrow V \\ S \wedge \neg V \\ \hline P \wedge \neg Q \end{array}$$

o)
$$\begin{array}{l} P \longrightarrow \neg Q \\ \neg P \longrightarrow (R \longrightarrow \neg Q) \\ (\neg S \vee \neg R) \longrightarrow \neg (\neg Q) \\ \neg S \\ \hline \neg R \end{array}$$

p)
$$\begin{array}{l} P \longrightarrow (Q \vee R) \\ Q \longrightarrow (S \vee T) \\ T \longrightarrow U \\ \neg (U \vee S) \\ \hline \neg P \end{array}$$

q)
$$\begin{array}{l} P \longrightarrow \neg Q \\ R \longrightarrow \neg Q \\ (S \vee T) \longrightarrow U \\ (\neg P \wedge \neg R) \longrightarrow S \\ \hline Q \longrightarrow U \end{array}$$

r)
$$\begin{array}{l} (P \vee Q) \wedge (R \vee S) \\ (P \longrightarrow R) \wedge (Q \longrightarrow S) \\ \neg R \\ \hline S \end{array}$$

$s)$
$$\begin{array}{l}(P \vee Q) \longrightarrow R \\ (R \vee Q) \longrightarrow [P \longrightarrow (S \longleftrightarrow T)] \\ P \wedge S \\ \hline S \longleftrightarrow T\end{array}$$

$t)$
$$\begin{array}{l}\neg S \longrightarrow Q \\ (U \vee P) \longrightarrow (V \vee T) \\ (R \wedge S) \longrightarrow T \\ \neg R \longrightarrow Q \\ Q \longrightarrow U \\ \hline \neg T \longrightarrow V\end{array}$$

$u)$
$$\begin{array}{l}\neg Q \longrightarrow \neg S \\ (\neg P \vee R) \vee \neg Q \\ S \\ \hline P \longrightarrow R\end{array}$$

$v)$
$$\begin{array}{l}R \wedge S \\ \neg P \longrightarrow \neg (S \vee R) \\ \neg Q \longrightarrow \neg P \\ \hline Q\end{array}$$

$w)$
$$\begin{array}{l}S \longrightarrow \neg P \\ R \longrightarrow Q \\ \neg (\neg P \wedge \neg R) \\ \hline S \longrightarrow Q\end{array}$$

$x)$
$$\begin{array}{l}(\neg S \vee P) \wedge (\neg P \vee R) \\ \neg R \vee Q \\ \hline S \longrightarrow Q\end{array}$$

$y)$
$$\begin{array}{l}(\neg A \longrightarrow B) \longrightarrow (P \wedge \neg R) \\ P \longrightarrow R \\ \hline \neg (A \vee B)\end{array}$$

12. Escriba una derivación para cada uno de los siguientes argumentos.

$a)$
$$\begin{array}{ll}(\forall\ x \text{ en U}) & \{[F(x) \vee H(x)] \to [G(x) \wedge K(x)]\} \\ \neg(\forall\ x \text{ en U}) & [K(x) \wedge G(x)] \\ \hline (\exists\ x \text{ en U}) & [\neg H(x)]\end{array}$$

$b)$
$$\begin{array}{ll}\neg(\forall\ x \text{ en V}) & [H(x) \vee K(x)] \\ (\forall\ x \text{ en V}) & \{[F(x)\ \vee \neg K(x)] \to \neg G(x)\} \\ \hline (\exists\ x \text{ en V}) & [G(x) \to L(x)]\end{array}$$

$c)$
$$\begin{array}{ll}\neg(\exists\ x \text{ en W}) & [P(x) \wedge Q(x)] \\ \neg(\exists\ x \text{ en W}) & [\neg R(x)] \\ (\exists\ x \text{ en W}) & \{R(x) \to [Q(x)\ \vee \neg S(x)]\} \\ \hline (\exists\ x \text{ en W}) & [S(x) \to \neg P(x)]\end{array}$$

$d)$
$$\begin{array}{ll}(\forall\ x \text{ en U}) & \{P(x) \to [\neg R(x) \vee S(x)]\} \\ (\exists\ x \text{ en U}) & [P(x) \to \neg S(x)] \\ \hline (\exists\ x \text{ en U}) & [P(x) \to \neg R(x)]\end{array}$$

$e)$
$$\begin{array}{ll}(\forall\ x \text{ en U}) & [R(x) \to C(x)] \\ \neg(\exists\ x \text{ en U}) & [T(x) \wedge \neg R(x)] \\ \hline (\forall\ x \text{ en U}) & [\neg C(x) \to \neg T(x)]\end{array}$$

$f)$
$$\begin{array}{ll}\neg(\exists\ a \text{ en V}) & [N(a) \wedge \neg B(a)] \\ (\exists\ b \text{ en V}) & [N(b) \wedge D(b)] \\ \hline (\exists\ c \text{ en V}) & [B(c) \wedge D(c)]\end{array}$$

$g)$
$$\begin{array}{ll}(\forall\ x \text{ en Z}) & \{[A(x) \to R(x)] \vee T(x)\} \\ (\exists\ x \text{ en Z}) & [T(x) \to P(x)] \\ \neg(\exists\ x \text{ en Z}) & [\neg A(x) \vee P(x)] \\ \hline (\exists\ x \text{ en Z}) & [R(x)]\end{array}$$

h)

$(\forall\ x$ en W$)(\exists\ y$ en W$)$	$\{E(x) \to [M(x) \vee N(y)]\}$
$\neg(\forall\ x$ en W$)$	$[M(y)]$
$\neg(\exists\ x$ en W$)$	$[\neg E(x)]$
$\neg(\forall\ x$ en W$)$	$[\neg N(x)]$

i)

$(\forall\ x$ en W$)(\exists\ y$ en W$)$	$\{E(x) \to [M(x) \vee N(y)]\}$
$\neg(\forall\ x$ en W$)$	$[M(x)]$
$(\forall\ x$ en W$)$	$[E(x)]$
$(\forall\ x$ en W$)$	$[N(x)]$

Capítulo 2

Estrategias de Prueba

2.1. Pruebas en Matemáticas.

La mayoría de los historiadores atribuyen a Tales de Mileto haber usado por primera vez las pruebas en el siglo VI antes de Cristo. De hecho, se presume que varios de sus aportes en Matemáticas se encuentran consignados en los trabajos de Euclides. Este último, quien vivió en Alejandría en el siglo III antes de Cristo, elaboró un compendio llamado *Los Elementos de Euclides*, sobre la geometría conocida en esa época y la escribe en forma axiomática. El trabajo de Euclides es quizas el primer tratado de la Matemática moderna, pues podría ser la primera vez que el racionamiento deductivo es usado para obtener propiedades elementales en el campo de la geometría.

Un sistema axiomático consiste en establecer unos principios básicos, llamados postulados o axiomas, y deducir a partir de ellos, por medio de pruebas rigurosas, los Teoremas, Proposiciones, Lemas o Corolarios, que en su conjunto conforman la teoría sobre determinada área de la Matemática. En la actualidad, prácticamente, todas las ramas de la Matemática son basadas en sistemas axiomáticos. La palabra "prueba" podría tener diferentes significados dependiendo del área de estudio. Por ejemplo, en Biología, Química o Física una prueba podría consistir en datos experimentales que confirmen cierta hipótesis. Intuitivamente en Matemáticas, una **prueba** es una sucesión de argumentos que muestran que una conclusión deseada se sigue lógicamente de las hipótesis dadas. Como ya habrán notado, el concepto de hipótesis en Matemáticas es completamente diferente al de otras áreas, para los matemáticos una hipótesis es una irformación que se tiene de antemano y para un físico, químico o biologo es algo que el cree que es cierto y desea comprobar realizando un experimento.

En este capítulo trataremos de entender como hacer una prueba, no como con las derivaciones que hemos hecho (que están más cerca de la lógica), sino como las pruebas que encontramos prácticamente en la mayoría de los libros de matemáticas. En la prueba no haremos dos columnas como lo veníamos haciendo en las derivaciones, sino que la prueba se desarrollará sin justificaciones lógicas de reglas de inferencia. Las justificaciones que se darán serán de orden matemático, refiriéndonos a axiomas o teoremas previos. Sin embargo, si analizamos en detalle la estructura de dichas pruebas veremos que allí detrás están las reglas de inferencia sosteniendolas.

En Matemáticas se prueban afirmaciones, que usualmente llamamos teoremas, proposiciones, lemas, corolarios y ejercicios. Todas estas afirmaciones necesitan ser probados con el mismo rigor, aunque algunas de ellas no tengan la misma importancia en la teoría. Los teoremas tienden a ser los resultados más importante; las proposiciones son usualmente menos importantes que los teoremas; los lemas son afirmaciones que son usadas para probar otros resultados; los corolarios son enunciados que se siguen fácilmente de otros resultados y los ejercicios son afirmaciones que son dejadas al lector para que las pruebe. A continuación mostramos el enunciado de un teorema que conocemos bastante bien: *el volumen V de una esfera de radio r es* $\frac{4\pi r^3}{3}$. Obsérvese que la expresión "$V = \frac{4\pi r^3}{3}$" no dice lo mismo que el enunciado que está en italicas. Es importante definir las variables, decir que V es el volumen de una esfera y que r es el radio. Realmente, esas son las hipótesis o premisas del teorema y por tanto es importante que queden definidas. Ahora, aunque las palabras "Si..., entonces..." no aparecen en dicho enunciado; este enunciado es realmente un condicional. En efecto rescribamoslo: "Si r y V son el radio y el volumen, respectivamente, de una esfera, entonces $V = \frac{4\pi r^3}{3}$". La mayoría de los teoremas, proposiciones, corolarios y lemas son de la forma $P \to Q$ o combinación de estos, aunque explícitamente no se vean las palabras "Si..., entonces...". Por tal motivo, antes de emprender la prueba de cualquier teorema, proposición, corolario o lema es necesario tener claro cuáles son las hipótesis o premisas y que es lo que se quiere probar. Es decir, debemos poder distinguir cual es P y cual es Q. Si bien las hipótesis del teorema constituyen P, ellas no son las únicas premisas que podemos usar en la prueba, pues todo teorema, definición o axioma establecido anteriormente, es válido como premisa. Las definiciones y axiomas nos permiten comenzar a trabajar en una teoría, pues si no estaríamos trabajando hacia atrás infinitamente.

La importancia de las pruebas debe ser mirada en su sitio correcto. No hay que exagerar, pues la intuición juega un papel interactivo con el rigor. La intuición y el rigor se retroalimentan mutuamente, sin este proceso los avances en Matemáticas serían prácticamente imposibles. Es la intuición la que señala los caminos, la que dice que puede ser importante en la investigación, pero son las pruebas rigurosas las que confirman o no, lo que señala la intuición. Al mismo tiempo las pruebas rigurosas hacen que la intuición se incremente y de esta manera ocurre la retroalimentación. Es decir, usamos las pruebas para convencernos de que algo es cierto, pero también las usamos porque haciéndolas se nos aclaran las ideas y probablemente se nos ocurren nuevas ideas.

Inicialmente para aprender a hacer pruebas las tendremos que hacer en un contexto que más o menos todos conozcamos, y el escogido va a ser la Teoría de Números intuitiva que tenemos. Supondremos que conocemos las principales propiedades de los números enteros, racionales o reales, es decir, sabemos que existen la suma, la resta, el producto, la división, la radicación y que además, conocemos las reglas de manejo de estas operaciones.

2.2. Pruebas Directas.

Si debemos probar $P \to Q$ una forma de hacerlo es suponer que P es cierto y avanzar deduciendo algunos hechos hasta que finalmente se llega a Q. Este estilo de prueba es lo que llamamos una prueba directa o por método directo.

Cuando se construye una prueba, primero se hace una exploración que nos aclarará cual es la mejor forma de escribir la prueba. Una cosa es la exploración y otra la prueba, una cosa es como se haya pensado la prueba y otra cosa es ya cuando se escribe. La prueba es el escrito final, que en general no muestra cómo se nos ocurrió la prueba. Algunas recomendaciones básicas para emprender la exploración es tener claro lo que se supone (*i.e., la hipótesis*) y tener claro lo que se quiere probar (*i.e., la tesis*). Observemos que al comenzar las pruebas que ya hicimos en la sección pasada, los primeros renglones establecían claramente lo que se supone y lo que se quiere probar. Esa es una buena práctica. Una vez se tiene esto claro se debe hacer la exploración. Ésta se hace comenzando por escoger una estrategia de prueba. Por ejemplo, se decide hacerla en forma directa y luego se debe imaginar cual será la prueba con dicha estrategia. Si no se logra imaginar los pasos para realizar la prueba, quizás es conveniente probar una estrategia diferente.

No hay una única manera de hacer una prueba, probablemente, se requerirá hacer muchas exploraciones, es decir, buscar ejemplos diversos que ayuden a entender que es lo que esta ocurriendo y ayuden a visualizar la prueba. De todas maneras la experiencia nos irá enseñando muchos trucos para hacer pruebas. Aún, si la estrategia ya está definida hay muchas maneras diferentes de proceder. Por ejemplo, para encontrar una prueba de $P \to Q$ uno comenzará asumiendo P, y avanzando lógicamente para tratar de llegar a Q. O puede que otro comience mirando a Q, y pensando que necesita para llegar a P e ir retrocediendo. O también se pueden combinar ambos métodos para encontrarse en la mitad. Esto anterior será sólo para entender los pasos que se deben dar en la prueba y será considerado un borrador. Finalmente el último paso de la prueba será la escritura. No importa cuan enredada haya sido la ruta para encontrar las ideas, la prueba escrita debe ser directa (si la estrategia era directa) y absolutamente lógica. Así, en una prueba directa se comenzaría así: Supongamos P... seguiría la argumentación paso a paso lógicamente... y finalmente se diría, entonces Q. El pensamiento intuitivo que nos ayuda a visualizar la prueba debe ser reemplazado por la deducción lógica en el momento de escribir. En resumen hay dos pasos principales en una prueba.

1. Formular la prueba en "borrador" (Exploración).
2. Escribirla correctamente.

De cómo se hagan estos dos pasos dependerá de muchos factores. En general los pasos (1) y (2) se retroalimentan y juegan un papel dialéctico. Haremos ahora un ejemplo y para esto daremos algunas definiciones.

Definición 2.1 (Número Par e Impar)**.** *Sean n un entero. Decimos que n es par si existe un entero k tal que $n = 2k$. Decimos que n es impar si existe un entero j tal que $n = 2j + 1$. Símbolicamente*

$$n \text{ es par} \iff (\exists k \text{ en } \mathbb{Z})(n = 2k)$$

$$n \text{ es impar} \iff (\exists j \text{ en } \mathbb{Z})(n = 2j + 1)$$

Hagamos un ejemplo de prueba directa

Teorema 2.2. *Sea n un entero. Entonces n es impar si existe un entero q tal que $n = 2q - 1$.*

Prueba: Supongamos que n es impar. Por definición existe j entero tal que $n = 2j + 1$. Definamos $q := j + 1$, el cual es un entero, pues la suma de dos enteros es un entero. Note además que

$$2q - 1 = 2(j + 1) - 1 = (2j + 2) - 1 = 2j + 1 = n.$$

Así pues, $n = 2q - 1$, lo que termina la prueba.

Definición 2.3 (Divisibilidad)**.** *Sean m y n enteros. Decimos que m divide a n si existe un entero q tal que $n = qm$. Si m divide a n escribimos $m|n$ y decimos también que m es un factor de n, y que n es divisible por m. Símbolicamente*

$$m|n \iff (\exists q \text{ en } \mathbb{Z})(n = qm)$$

Observese que "$m|n$" es una afirmación y no un número, además, involucra el cuantificador existencial.

Teorema 2.4. *Sean a, b y c enteros. Si $a|b$ y $b|c$ entonces $a|c$.*

Borrador: Como nuestro objetivo es probar que $a|c$, de alguna manera debemos encontrar un entero q que cumpla que $aq = c$. Utilizando el hecho de que $a|b$ y $b|c$, sabemos que existen enteros r y s tales que $ar = b$ y $bs = c$. Esto nos sugiere tomar $q = rs$, lo cual vemos que sí funciona pues $(ar)s = a(rs) = c$. Escribamos ahora sí la prueba.

Prueba: Supongamos que $a|b$ y $b|c$. Entonces existen enteros r y s tales que $ar = b$ y $bs = c$. Definamos $q := rs$. Luego $aq = a(rs) = (ar)s = bs = c$. Por tanto $aq = c$, lo que implica que $a|c$. □

Obsérvese que en esta prueba estamos haciendo dos ejemplificaciones existenciales y por eso usamos las letras diferentes r y s. Veamos otra prueba.

Teorema 2.5. *Sea n un número entero. Entonces*

1. *Si n es par, entonces $3n$ es par.*

2. *Si n es impar, entonces $3n$ es impar.*

Borrador: Sabemos que n es un número par, esto quiere decir que existe un número entero k tal que $n = 2k$ y queremos probar que $3n$ también es par; es decir, que hay un número entero q tal que $3n = 2q$. Esto nos sugiere tomar a q como $3k$. Efectivamente vemos que $3n = 3(2k) = 2(3k)$. Ahora sí, escribamos la prueba.

Prueba: Sea n un entero par, luego $n = 2k$, para algún entero k. Si definimos $q := 3k$, entonces $3n = 3(2k) = 2(3k) = 2q$, lo que implica que $3n$ es par. La prueba de la segunda parte del teorema es dejada como ejercicio al lector. □

2.3. Pruebas por Contrarrecíproco y Contradicción.

Estudiaremos dos clases de pruebas que aunque parezcan más complicadas, muchas veces nos permiten resolver problemas de manera más fácil.

Método del Contrarrecíproco.

Consiste en que para mostrar $P \to Q$ mejor se prueba "$\neg Q \to \neg P$" y esto último lo hacemos de forma directa. Por ejemplo

Teorema 2.6. *Sea n un número entero. Si n^2 es par, entonces n es par.*

Borrador: Hacer esta prueba por método directo es muy duro, trate de hacerla. Queremos mostrar que n es par, esto es, que existe q entero tal que $n = 2q$. Vamos a suponer que n no es par, entonces n es impar (mostraremos mas adelante que un entero no puede ser par e impar simultáneamente), luego $n = 2m + 1$, para algún entero m. Lo que se nos viene a la mente es remplazar en n^2. Entonces $n^2 = (2m + 1)^2 = 2m^2 + 4m + 1 = 2(2m^2 + m) + 1$. Lo que estamos diciendo es que n^2 es impar, lo cual contradice el hecho que n^2 es par. Escribamos la prueba.

Prueba: Debemos probar que si n^2 es un entero par, entonces n es par. Lo haremos por contrarrecíproco, para esto supongamos que n no es par, es decir, n es impar y probaremos que n^2 no es par. Como n es impar existe un entero k tal que $n = 2k+1$, luego $n^2 = (2k+1)^2 = 2(2k^2+2k)+1 = 2q+1$, donde $q := 2k^2 + 2k$ es claramente un entero. De aquí tenemos que n^2 es impar, lo que termina la prueba. □

El Método de Contradicción o Absurdo.

Consiste en lo siguiente, para probar $P \to Q$ probaremos que $\neg(\neg(P \to Q))$ es cierto, lo cual hacemos aprovechando la equivalencia $\neg(P \to Q) \Leftrightarrow P \wedge \neg Q$, y se trata de probar que si $P \wedge \neg Q$ es verdadero se deriva una contradicción, luego obligatoriamente $\neg(P \to Q)$ es falso y por lo tanto concluiremos que $\neg(\neg(P \to Q))$ debe ser verdadero. Observe que usamos Doble Negación y el Principio del Medio Excluído. Veamos un ejemplo.

Teorema 2.7. *No existe un entero n que sea par e impar simultáneamente.*

Prueba: Supongamos que n es para e impar, entonces existen k y j enteros tales que $n = 2k$ y $n = 2j + 1$. Luego $2k = 2j + 1$, lo que implica que $k - j = \frac{1}{2}$, pero sabemos que la diferencia de dos enteros es un entero, lo que implica que $\frac{1}{2}$ es un entero, pero esto es absurdo. Lo que termina la prueba del teorema. □

Veamos otro ejemplo, pero antes necesitamos una definicón.

Definición 2.8 (Números Irracionales)**.** *Sea x un número real. Decimos que x es un número racional si existen un entero m y un natural n tales que $x = \frac{m}{n}$. Si x no es un racional, diremos que x es irracional.*

Teorema 2.9. $\sqrt{2}$ *es irracional.*

Prueba: Supongamos que $\sqrt{2}$ es racional. Entonces existen m entero y n natural tales que $\sqrt{2} = m/n$. De hecho, podemos asumir que la fracción $\frac{m}{n}$ está escrita en la forma reducida, esto es, que m y n no tienen otro factor común diferente del 1. Como $\sqrt{2}$ es positivo, tenemos que m es un natural. Luego $2 = \frac{m^2}{n^2}$, esto es, $m^2 = 2n^2$. Lo que indica que m^2 es par, por ejemplo anterior se tiene que m es par. Así que existe q en los enteros tal que $m = 2q$. Por tanto $(2q)^2 = 2n^2$, es decir $n^2 = 2q^2$, lo que nos dice que n^2 es par, así que existe p entero tal que $n = 2p$. Por tanto m y n tienen como factor común al 2, lo cual es absurdo pues la representación de $\sqrt{2}$ es la más reducida. □

2.4. Método de Casos y Pruebas de "si y sólo si".

Método de Casos o Disyunción de Casos.

El método de casos o disyunción de casos lo usamos cuando tenemos que probar, por ejemplo, algo de la forma $(A \vee B) \to Q$ y por ejercicio anterior esto es equivalente a probar $(A \to Q) \wedge (B \to Q)$ o también por las reglas de inferencia se tiene que

A	$\vee$	B	
A	$\to$	Q	
B	$\to$	Q	
Q	$\vee$	Q	Dilema Constructivo
	Q		$Q \vee Q \Leftrightarrow Q$ es una tautología

Es claro que el argumento dado arriba puede ser generalizado para probar algo de la forma $(A \vee B \vee C) \to Q$. Para hacer algunos ejemplos de este método de demostración, primero se hará un resumen sobre desigualdades en los números reales.

Propiedades de la desigualdad sobre los números reales.

1. (Tricotomía) Sean x, y números reales arbitrarios. Entonces una y sólo una de las siguientes afirmaciones se satisface $x < y$, $y < x$ ó $x = y$.
2. (Monotonía de la suma) Sean x, y y z números reales arbitrarios. Si $x < y$, entonces $x+z < y+z$
3. (Transitividad) Sean x, y y z números reales arbitrarios. Si $x < y$ y $y < z$, entonces $x < z$
4. (Monotonía del producto) Sean x, y y z números reales arbitrarios. Si $x < y$ y $0 < z$, entonces $xz < yz$.

A continuación enunciamos dos resultados que serán usados de aquí en adelante y son dejados como ejercicios al lector

Teorema 2.10. *1. Sean a, b y c números reales. Si $a < b$, entonces $a - c < b - c$.*

2. Sean a, b y c números reales. Si $a < b$ y $z < 0$, entonces $ac > bc$.

Ahora veamos un ejemplo sencillo.

Teorema 2.11. *Sean a y b números reales. $a^2 < b^2$ si $0 < a < b$ ó si $b < a < 0$.*

Prueba: Supongamos que a y b son números reales. Veamos que tanto si $0 < a < b$ como si $b < a < 0$, tenemos que $a^2 < b^2$. Es decir, en ambos casos debemos probar que $a^2 < b^2$. En efecto, si $0 < a < b$ entonces $b > 0$ y $a < b$, luego $ab < bb$, pues al multiplicar una desigualdad en ambos lados por algo positivo la desigualdad no cambia y, similarmente, como $a > 0$ y $a < b$ entonces $aa < ab$, luego por transitividad, $aa < bb$, es decir $a^2 < b^2$ es cierto.
Consideremos ahora el otro caso. Si $b < a < 0$ entonces $0 < -a < -b$, pues al multiplicar una desigualdad por número negativo ella cambia y por el caso anterior tendríamos que $(-a)^2 < (-b)^2$, pero por propiedades conocidas $(-a)^2 = a^2$ y $(-b)^2 = b^2$, luego $a^2 < b^2$ también es cierto. En ambos casos se concluye que $a^2 < b^2$, lo que termina la prueba. □

Ejemplo 2.12. *Volvamos a analizar el teorema que acabamos de probar. Este dice así: Sean a y b números reales. $a^2 < b^2$ si $0 < a < b$ ó si $b < a < 0$.*

Vemos que este teorema tiene la forma $P \vee Q \to R$ siendo,
P : a y b números reales tales que $0 < a < b$.
Q : a y b números reales tales que $b < a < 0$.
R : $a^2 < b^2$.

La hipótesis es	$P \vee Q$	
Probamos que	$P \to R$	
y que	$Q \to R$	
y concluimos	$R \vee R$	Por dilema constructivo.

Pero $R \vee R \Leftrightarrow R$. Las reglas de inferencia siempre estarán allí, aunque no se vean explícitamente.

Ejemplo 2.13. *Sea n un entero, entonces uno de estos dos números n y $n + 1$ es par, y el otro es impar.*

Borrador Reescribamos el enunciado. Sea n un entero, entonces si uno de los números n ó $n+1$ es par, entonces el otro es impar. Analizaremos los dos casos posibles. Ya sea que n es par o que $n + 1$ es par y en cada caso debemos concluir que el otro es impar.

Prueba: Sea n un entero. Entonces analicemos los dos casos.
Caso 1: Si n es par, entonces existe k entero tal que $n = 2k$, luego $n + 1 = 2k + 1$ y así $n + 1$ es impar.

Caso 2: Si $n+1$ es par, entonces existe r entero tal que $n+1 = 2r$, luego $n = 2r-1 = 2(r-1)+2-1 = 2(r-1)+1$, por tanto n es impar. □

En el ejemplo anterior teníamos sólo dos casos posibles, pero a veces hay que analizar más de dos casos, y en todos se debe llegar a la misma conclusión. Se necesita que los casos analizados cubran todas las posibilidades.

Nota 2.14. *Si queremos probar $P \to (A \vee B)$ este no es por casos. Podemos usar $(\neg A \wedge \neg B) \to \neg P$ (contrerrecíproco) o, también que $[P \to (A \vee B)] \Leftrightarrow [(P \wedge \neg A) \to B]$. Entonces podría ser por método directo probando $(P \wedge \neg A) \to B$.*

Teorema 2.15. *Sean x, y números reales. Si xy es irracional, entonces x es irracional o y es irracional.*

Borrador El teorema tiene la forma $P \to (A \vee B)$. Supondremos $P \wedge \neg A$ para tratar de concluir B. Es decir supondremos que xy es irracional y x es racional, y debemos llegar a que y es racional.

Prueba: Supongamos que xy es un número irracional y que x es racional. Entonces existen m un entero y n un natural tales que $x = \frac{m}{n}$. Debemos probar que y es irracional. Usemos el método de contradicción. Supongamos que y es racional, entonces existen un entero r y un natural s tales que $y = \frac{r}{s}$. Luego $xy = (\frac{m}{n})(\frac{r}{s}) = \frac{mr}{ns}$, pero mr es un entero y ns es un natural, por tanto xy es racional, lo cual es absurdo. Así que y es irracional. □

Nota 2.16.
1. *¿Cómo probamos teoremas de la forma $A \wedge B \to P$? Se supone $A \wedge B$ y se llega a P. No es necesario usar el método de casos.*
2. *¿Y para probar una afirmación como $P \to A \wedge B$? Observemos las siguientes equivalencias: $[P \to (A \wedge B)] \Leftrightarrow [(P \to A) \wedge (P \to B)] \Leftrightarrow [(\neg A \vee \neg B) \to \neg P]$. La última afirmación la podemos demostrar usando el método de casos.*

Pruebas con "si y sólo si".

Probar $P \leftrightarrow Q$ es equivalente a probar $(P \to Q) \wedge (Q \to P)$ y estos dos condicionales los probaremos por cualquiera de los métodos explicados anteriomente. A continuación presentamos un ejemplo.

Teorema 2.17. *Sean a y b enteros diferentes de cero. Entonces $a|b$ y $b|a$ si y sólo si $a = b$ ó $a = -b$.*

Prueba: Sean a y b dos enteros distintos de cero.
"$\Rightarrow$" Supongamos que $a|b$ y $b|a$. Entonces existen enteros m y n tales que $am = b$ y $bn = a$. Usando las dos igualdades anteriores tenemos que $(bn)m = b$. Luego $b(nm) = b$ y como $b \neq 0$ entonces $nm = 1$. Lo que implica que $n = 1$ y $m = 1$ ó $n = -1$ y $m = -1$. En el primer caso tendríamos que $a = b$ y en el segundo caso que $a = -b$.
"$\Leftarrow$" Supongamos ahora que $a = b$ ó que $a = -b$ Examinemos cada caso. Si $a = b$ entonces claramente $a1 = b$ y así $a|b$ pero también $a = b1$ y entonces también $b|a$. Y si $a = -b$ entonces $a(-1) = b$ y en este caso $a|b$ y también $a = (-1)b$ luego $b|a$. □

Veamos otro ejemplo.

Teorema 2.18. *Sean m y n enteros. Entonces mn es impar si y sólo si m y n son ambos impares.*

Borrador. Probemos la implicacion "$\Leftarrow$" en forma directa y la implicación "$\Rightarrow$" por contrarrecíproco y disyunción de casos.

Prueba: Sean m y n enteros.
"$\Leftarrow$" Supongamos que m y n son ambos impares, luego existen enteros r y s tales que $m = 2r + 1$ y $n = 2s + 1$ entonces $mn = (2r + 1)(2s + 1) = 4rs + 2r + 2s + 1 = 2(2rs + r + s) + 1$. Ahora, defina $q := 2rs + r + s$ y note que q es un entero, pues r y s lo son. Por tanto $mn = 2q + 1$ y consecuentemente mn es impar.
"$\Rightarrow$" Razonemos por contradicción. Supongamos que n y m no son ambos impares. Es decir estamos suponiendo que m es par o que n es par. Analicemos cada caso.
Caso 1: Si m es par, entonces existe un k entero tal que $m = 2k$, luego

$$mn = (2k)n = 2(kn)$$

y como k y n son enteros, kn también lo es, luego mn no es impar.
Caso 2: Si n es par se prueba de forma similar al Caso 1 que mn no es impar.
Luego hemos probado que si m y n son ambos impares entonces mn no es impar, así que por contrarrecíproco el resultado es cierto. □

Teorema 2.19. *Sea n un entero. Entonces n es impar si y sólo si existe un entero q tal que $n = 2q-1$.*

Prueba: La prueba se deja como ejercicio, note que ya se hizo una dirección en el Teorema 2.2 □

Es muy común encontrar teoremas donde se quiere probar que varias afirmaciones son equivalentes. La forma de ellos es: Se dan hipótesis y se dice al final de las hipótesis: "Entonces las siguientes afirmaciones son equivalentes".

(1) A
(2) B
(3) C
(4) D

Para hacer la prueba es suficiente hacer un círculo que pase por todas las afirmaciones. Por ejemplo podríamos probar (1)⇒(2), luego (2)⇒(4), después (4)⇒(3) y finalmente (3)⇒(1) y al cerrar el círculo quedaron probadas todas las equivalencias. Cada una de las implicaciones se demuestra con cualquiera de las métodos aprendidos. También se podría mostrar que (1)⇒(4), después (4)⇒(2), luego (2)⇒(3) y finalmente que (3)⇒(1). Como dijimos anteriormente, es sólo hacer implicaciones que formen un círculo.

2.5. Cuantificadores en Teoremas.

Si miramos de cerca algunas de las pruebas mostradas anteriormente (sino todas) nos daremos cuenta de que ellas involucran cuantificadores. La presencia de ellos es una de las mayores fuentes de error si no se trabaja con cuidado. Comencemos considerando afirmaciones que involucran un solo cuantificador universal, esto es, son aquellos de la forma $(\forall x \text{ en } U)P(x)$. Algunos de los teoremas explicados en este libro tienen esta forma.

Ejemplo 2.20. *"Sea n un entero. Entonces n^2+n es par". Lo podemos entonces reformular "Para todo n en los enteros, n^2+n es par". Para hacer la prueba, lo que hacemos es tomar un entero cualquiera que denotamos por n y para este entero cualquiera se llega a la conclusion de que n^2+n es par. Y así queda probada la afirmación para todo entero n.*

Recordemos que la exploración no es la prueba y si bien en la exploración podríamos haber chequeado que 3^2+3 es par, esto no constituye la prueba para todos los enteros n.

¿Cómo probar $(\forall x \text{ en } U)P(x)$? Pues se prueba su equivalente "Si x esta en U, entonces $P(x)$ es verdad" que es un condicional y lo podemos probar con cualquier método. Así pues, tomamos un elemento arbitrario x en U y se trata de probar que $P(x)$ es verdadero. Si hacemos esto, entonces queda probado $(\forall x \text{ en } U)P(x)$. ¿Qué reglas de inferencia hay detrás? Generalización Universal, pues se probó $P(x)$ con x arbitrario y de allí se concluye $(\forall x \text{ en } U)P(x)$.

Otro tipo de teorema es aquel que involucra un único cuantificador existencial y tiene la forma $(\exists x \text{ en } U)P(x)$. Para probar un teorema de esta forma, se trata de producir (de alguna forma la cual resulta irrelevante en el teorema) un elemento particular z_0 en U que verifique a $P(x)$, es decir, tal que $P(z_0)$ es verdad. En esta prueba también hay un condicional que podemos probar con cualquiera de los métodos. Ellas tienen más o menos la siguiente estructura. Primero de alguna forma se define un z_0 en U escogido de tal manera que uno sepa que va a cumplir $P(x)$, luego se prueba el condicional "Si $x=z_0$ entonces $P(x)$ es verdad". La forma de cómo se encuentra el z_0 es irrelevante en la prueba, pero muy importante en la exploración. Muchas veces para encontrar el objeto supondremos que $P(z_0)$ es verdadero y se va hacia atrás para identificar a z_0. Pero ésta no es la prueba, pues no siempre es posible reversar los argumentos. Hagamos un ejemplo, para lo cual necesitamos una definición preliminar.

Definición 2.21. *Recordemos que si* $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *entonces* $\det A = ad-bc$ *y* $\mathrm{Tr}A = a+d$.

Proposición 2.22. *Existe una matriz A de tamaño 2×2 con entradas enteras tal que* $\det A = 4$ *y* $\mathrm{Tr}A = 7$.

Borrador. Debemos exhibir un matriz A que cumpla esas dos características. Con que mostremos una es suficiente, pero podría haber muchas.

Suponga que $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Las condiciones $\det A = 4$ y $\mathrm{Tr}A = 7$, implican $ad-bc=4$ y $a+d=7$,

respectivamente. Como a y d son enteros las opciones para a y d son muchas. Les damos valores y luego tanteando buscamos los valores para b y c. Por ejemplo $a = 3$, $d = 4$, luego $ad = 12$, entonces $bc = 12 - 4 = 8$ y podríamos escoger a $b = 1$ y $c = 8$ y, así, $A = \begin{pmatrix} 3 & 1 \\ 8 & 4 \end{pmatrix}$ es una matriz que cumple las condiciones pedidas. En realidad hay muchas pero para probar la proposición necesitamos mostrar sólo una.

Prueba: Considere $A = \begin{pmatrix} 3 & 1 \\ 8 & 4 \end{pmatrix}$. Entonces $\det A = 3 \times 4 - 1 \times 8 = 4$ y $\mathrm{Tr}A = 3 + 4 = 7$. Lo que termina la prueba. □

Obsérvese la diferencia entre el borrador y la prueba. En el borrador salimos de lo que queríamos concluir hacia atrás, pero eso no es la prueba. Y aunque uno ve que pueden haber muchas matrices que verifican las condiciones, es suficiente mostrar una.

Cuidados que debemos tener.

Al resolver una ecuación; lo que se muestra es la forma como se encontró el x que cumple la condición, pero estrictamente hablando no es una prueba.

Ejemplo 2.23. *Si $x + 3 = 2$, luego $x = 2 - 3$, así $x = -1$.*

Lo que queremos probar es:

Proposición 2.24. *"Existe un x en los reales tal que $x + 3 = 2$".*

Prueba: Sea $x = -1$, entonces reemplazando $x = -1$ en $x + 3 = 2$ obtenemos $-1 + 3 = 2$, luego $x = -1$ verifica la ecuación. □

Sin embargo pedagógicamente, a nivel elemental, se exige que el estudiante muestre el procedimiento para encontrar que $x = -1$.

Volviendo a teoremas que tienen el cuantificador existencial, es común encontrar teoremas que exigen probar que es único el objeto que verifica lo que queremos. En nuestra proposición de la matriz veíamos que eran varias las matrices que podían satisfacer la propiedad. Pero algunas veces es un sólo objeto y se puede probar que ese es el único, estos teoremas los llamamos de **existencia y unicidad**. A continuación presentamos las propiedades más importantes de las funciones exponencial y logaritmo natural, las cuales serán necesarias en los siguientes ejemplos.

1. Sean x y y números reales, entonces $e^x e^y = e^{x+y}$.
2. Sea x un número real, entonces $e^x > 0$, $e^0 = 1$ y $\ln 1 = 0$.
3. $\ln(xy) = \ln x + \ln y$, para todo los números reales $x, y > 0$.
4. $e^{\ln x} = x$, para todo número real $x > 0$.

5. $\ln(e^x) = x$, para todo número real x.

6. Si $a > 0$ y r es un número real, entonces $\ln(a^r) = r \ln a$.

7. Sean x, y números reales. Si $e^x = e^y$, entonces $x = y$, esto quiere decir que la función exponencial es inyectiva, concepto que definiremos más adelante

8. Sean x, y números positivos. Si $\ln x = \ln y$, entonces $x = y$, esto quiere decir que la función logaritmo natural es inyectiva en $(0, +\infty)$.

Proposición 2.25. *Existe un único x en los reales tal que*

$$e^{x+3} = 2. \tag{2.1}$$

Borrador Si $e^{x+3} = 2$ entonces $\ln e^{x+3} = \ln 2$, luego $x + 3 = \ln 2$, así que, $x = \ln 2 - 3$. Con esto hemos identificado un real especifico que satisface la ecuación. Ahora, para probar la unicidad, supongamos que hay otro elemento y que satisface la condición, es decir, tal que $e^{y+3} = 2$, pero haciendo los mismos cálculos se llega a que $y = \ln 2 - 3$ luego es el único objeto que satisface la ecuación (2.1).

Prueba: Unicidad: Supongamos que existen dos números a y b tales que $e^{a+3} = 2$ y $e^{b+3} = 2$. Entonces $e^{a+3} = e^{b+3}$, luego por la inyectividad de la función exponencial se tiene que $a + 3 = b + 3$ y así $a = b$.
Existencia: Sea $x = \ln 2 - 3$ reemplazando en la ecuación (2.1) obtenemos que $e^{(\ln\ 2-3)+3} = e^{\ln\ 2} = 2$. Luego x verifica (2.1). □

Recordemos que

$$\neg[(\forall x \text{ en } U)P(x)] \Leftrightarrow (\exists x \text{ en } U)(\neg P(x))$$

y que

$$\neg[(\exists x \text{ en } U)P(x)] \Leftrightarrow (\forall x \text{ en } U)(\neg P(x)).$$

Entonces si queremos probar por ejemplo que $(\forall x \text{ en } U)P(x)$ es una afirmación falsa es suficiente probar que $(\exists x \text{ en } U)(\neg P(x))$ y esta última la haríamos como ya hemos mostrado, es decir encontrando un elemento x_0 en U que no satisface a $P(x)$. Dicho elemento lo llamamos **Contraejemplo**.

Por ejemplo para mostrar que la afirmación "Para todo número real x se tiene que $x + 1 = 0$" es falsa, basta encontrar un contraejemplo. Esto es falso pues $x = 8$ es un número real y sin embargo $x + 1 = 8 + 1 = 9 \neq 0$. Así que $x = 8$ es un contraejemplo.

¿Cómo enfrentar pruebas con más de un cuantificador? La clave es tomarlos uno por uno de afuera hacia adentro, y si ellos no están explícitos se debe tener especial cuidado en no confundir su orden.

Proposición 2.26. *Para cada número real x existe un numero real $y > 0$ tal que $e^x - y > 0$*

Borrador La proposición tiene la forma $(\forall x \text{ en } \mathbb{R})(\exists y > 0)(e^x - y > 0)$. Si $P(x) = (\exists y > 0)(e^x - y > 0)$ lo que hay que probar es $(\forall x \text{ en } \mathbb{R})P(x)$. Entonces se trata de dar un real arbitrario x

para el cual debemos probar que $P(x) = (\exists y > 0)(e^x - y > 0)$ es verdadero y esta última la podremos probar si encontramos un y_0 real que verifique dicha desigualdad, dicho y_0 puede depender de x. Como $e^x > 0$, entonces si definimos $y_0 = \frac{e^x}{2} > 0$ vemos que se cumple la desigualdad.

Prueba: Sea x un número real arbitrario. Considere $y_0 = \frac{e^x}{2}$ y note que

$$e^x - y_0 = e^x - \frac{e^x}{2} = \frac{e^x}{2} > 0,$$

pues $e^x > 0$. Luego para cada real x hemos encontrado un número real y_0 positivo tal que $e^x - y_0 > 0$. Lo que prueba la proposición. □

En contraposición con la proposición anterior, la afirmación "existe un número real positivo y tal que $e^x - y > 0$, para todo real x" es falsa. En efecto ella tiene la forma $(\exists y > 0)(\forall x \text{ en } \mathbb{R})(e^x - y > 0)$. Si probamos que $(\forall y > 0)(\exists x \text{ en } \mathbb{R})(e^x - y \leq 0)$ es cierto entonces tendríamos que su negación es falsa. Escribamos esto como una proposición.

Proposición 2.27. *Para todo real positivo y existe un real x tal que $e^x - y \leq 0$.*

Prueba: Sea y un número positivo arbitrario. Entonces $\ln y$ existe. Sea $x_0 = \ln y - 1$, entonces $x_0 < x_0 + 1 = \ln y$ y como la función exponencial es creciente se tiene que $e^{x_0} < e^{\ln y}$. Luego $e^{x_0} < y$ y así $e^{x_0} - y < 0$ lo que implica que $e^{x_0} - y \leq 0$. Hemos entonces probado que para todo y real positivo existe un x_0 real tal que $e^{x_0} - y$ es menor o igual que cero. Luego la afirmación "existe un número real positivo y tal que $e^x - y > 0$, para todo real x" es falsa. □

Proposición 2.28. *Existe un real positivo y tal que para todo número real x se tiene $x^2 + 1 > y$.*

Borrador La afirmación es de la forma $(\exists y > 0)(\forall x \text{ en } \mathbb{R})(x^2 + 1 > y)$. Bastará encontrar un $y_0 > 0$ que verifica que $(\forall x \text{ en } \mathbb{R})(x^2 + 1 > y_0)$, como $x^2 + 1 \geq 1$ si tomamos cualquier y tal que $0 < y < 1$, la prueba estaría terminada.

Prueba: Sea $y_0 = \frac{1}{2}$, entonces $0 < y_0 < 1$. Ahora, considere x un real arbitrario, entonces $x^2 \geq 0$, luego $x^2 + 1 \geq 1$ y como $1 > \frac{1}{2} = y_0$ entonces ${x_0}^2 + 1 \geq y_0$. Lo que termina la prueba de la proposición. □

Definiremos ahora lo que son los números primos y compuestos, conceptos que serán útiles para hacer algunos ejercicios.

Definición 2.29 (Números Primos)**.** *Sea n un entero positivo mayor que 1. Decimos que n es primo si los únicos divisores positivos que tiene son el 1 y él mismo. Diremos que un entero positivo mayor que 1 es compuesto si no es primo. Por convenio 1 no es primo y tampoco compuesto.*

De la definición anterior se tiene que si m es un entero positivo, n es primo y $m|n$, entonces $m = 1$ ó $m = n$. También se deduce que si n es compuesto, existen enteros positivos p y q tales que $p \neq 1, p \neq n$ y $n = pq$.

2.6. Escribiendo Matemáticas

Cuando escribimos debemos pensar que habrá lectores diferentes a nosotros. Por lo tanto las cosas deben estar escritas clara y correctamente. Por eso debemos seguir las siguientes reglas

1. Una prueba escrita se debe defender sola. No asuma que quien lee es un genio. Piense que usted no está al lado de quien lee para explicarle lo que usted quiere decir.

2. Escriba de manera precisa y cuidadosa. Esté seguro de que lo que escribe es lo que usted quiere decir. Por ejemplo, no olvide poner comas y puntos donde debe colocarlos. No olvide las hipótesis al redactar los teoremas. Revise sus escritos como si fuera otro el que lee.

3. Pruebe lo que es apropiado. Que no le falten detalles importantes, pero tampoco exagere en las justificaciones.

4. Sea cuidadoso con expresiones como "Es obvio que". Lo que le puede parecer obvio a usted, puede que a otra persona no le parezca. En inglés: Obvious, es algo cuya demostración en tiempo no requiere mucho esfuerzo. Trivial (en inglés) es algo que si bien puede tomar mucho tiempo para probar, una vez se encuentra la prueba es fácil.

5. Use frases completas y gramaticalmente correctas.

6. Use los signos de igualdad correctamente.

 Ejemplo 2.30. *Se pide encontrar $f'(x)$ para $f(x) = x^2$ y el estudiante escribe "$f(x) = x^2 = 2x = f'(x)$", esto no tiene sentido. O si escriben "$f(x) = x^2$, entonces $2x$" tampoco es correcto. El signo de igualdad lo están usando incorrectamente. Hay que pensar que "=" significa "es igual" y por tanto no se puede poner en cualquier parte, ni se debe dejar de poner donde se necesite.*

7. Defina todos los símbolos y términos que usa. Es importante definir el significado que tienen las letras que usa y las palabras nuevas que se usan. Trate de no inventar nuevos términos, más de lo necesario, y de que las letras sean lo más sencillas posibles, trate de que no haya muchos subíndices o superíndices. Hágale la vida fácil al que lee.

8. Divida una prueba muy larga en pasos o extraiga lemas.

9. Distinga el lenguaje formal del informal.
 Lenguaje formal: definiciones, afirmaciones, teoremas, pruebas. En inglés la palabra "formal" significa que el procedimiento se hará asumiendo todas las hipótesis que se necesiten. Un significado un poco different al que usamos en el castellano.
 Lenguaje informal: se usa para motivación o intuición.

10. Otras recomendaciones.

 a) No ponga un símbolo inmediatamente después de un signo de puntuación. Use alguna palabra entre los dos.

 b) En la escritura final no use símbolos como $\forall$,$\exists$, $\wedge$, $\vee$, $\neg$. Use palabras.

c) Use notación consistente, por ejemplo, si comienza denotando las matrices con mayúsculas, sígalas denotando con mayúsculas.

d) Escriba fórmulas largas en una sola línea reservada para ellas, pero entienda que es la continuación de lo que escribe.

e) Ponga mayúsculas cuando va a referirse a teoremas, proposiciones o capítulos que tienen un número, por ejemplo: "Según el Teorema 2.2.3...", pero no ponga mayúsculas en frases como: "el teorema anterior dice".

2.7. Ejercicios

1. Pruebe el Teorema 2.10.
2. Sean n y m enteros.
 (i) Muestre que $1|n$.
 (ii) Muestre que $n|n$.
 (iii) Muestre que si $m|n$, entonces $m|(-n)$.
3. Sea n un entero.
 (i) Muestre que si n es par, entonces $3n$ es par.
 (ii) Muestre que si n es impar, entonces $3n$ es impar.
4. Sea n un entero. Muestre que si n es par entonces n^2 es par, y si n es impar entonces n^2 es impar.
5. Sea n un entero. Decimos que n es múltiplo de 3 si $n = 3k$ para algún entero k. Sean n y m enteros.
 (i) Suponga que n y m son múltiplos de 3. Muestre que $n + m$ es múltiplo de 3.
 (ii) Suponga que n es múltiplo de 3. Muestre que nm es múltiplo de 3.
6. Sean $a,\ b,\ c,\ m$ y n enteros. Muestre que si $a|b$ y $a|c$, entonces $a|(bm + cn)$.
7. Sea $a,\ b,\ c$ y d enteros. Muestre que si $a|b$ y $c|d$, entonces $ac|bd$.
8. Sean a y b enteros. Muestre que si $a|b$, entonces $a^n|b^n$ para todo entero positivo n. (No se necesita inducción matemática en este ejercicio)
9. Sea n un entero. Muestre que si n^2 es impar, entonces n es impar.
10. Sean $a,\ b$ y c enteros. Muestre que si a no divide a bc, entonces a no divide a b.
11. Muestre que el producto de un número racional diferente de cero y un número irracional es irracional.
12. Sean $a,\ b$ y c enteros. Suponga que existe un entero d tal que $d|a$ y $d|b$, pero d no divide a c. Muestre que la ecuación $ax + by = c$ no tiene soluciones tales que x y y sean enteros.

13. Sea n un entero compuesto. Muestre que existen enteros p y q tales que $n = pq$, y $1 < p, q < n$.

14. Sea $c > 2$ un entero compuesto. Muestre que existe un entero positivo $b \neq 1$ tal que $b|c$ y $b \leq \sqrt{c}$. (Haga esta prueba en forma directa).

15. Sea q un entero positivo tal que $q \geq 2$ y para todo a y b enteros, si $q|ab$ entonces $q|a$ o $q|b$. Muestre $\sqrt{q}$ es irracional.

16. Sea q un entero positivo tal que $q \geq 2$ y para todo a y b enteros, si $q|ab$ entonces $q|a$ o $q|b$. Muestre que q es un número primo (el recíproco de esta afirmación también es verdadero, pero es mucho más difícil de probar).

17. Sean $a,\ b$ y c enteros tales que $c \neq 0$. Muestre que $a|b$ si y sólo si $ac|bc$.

18. Sean a y b enteros. Decimos que a y b son **primos relativos** si la siguiente condición se cumple: Si n es un entero tal que $n|a$ y $n|b$, entonces $n = \pm 1$.

 (1) Encuentre dos enteros a y b que sean primos relativos. Encuentre dos enteros c y d que no sean primos relativos.

 (2) Suponga que a y b son enteros positivos. Muestre que las siguientes afirmaciones son equivalentes.

 (i) a y b son primos relativos.

 (ii) $a + b$ y b son primos relativos.

 (iii) a y $a + b$ son primos relativos.

19. Sea n un entero. Muestre que uno de los dos números n y $n + 1$ es par, y el otro es impar.

20. Asuma que si n es un entero, entonces exactamente una de las siguientes afirmaciones es válida: $n = 3k$ para algún entero k, ó $n = 3k + 1$ para algún entero k, ó $n = 3k + 2$ para algún entero k. (La prueba de este hecho es basado en el Algoritmo de la División que probaremos más adelante.) Sean n y m enteros.

 (1) Suponga que n es múltiplo de 3 y que m no es múltiplo de 3. Muestre que $n + m$ no es múltiplo de 3.

 (2) Muestre que mn es múltiplo de 3 si y sólo si m ó n es múltiplo de 3.

21. Encuentre todas las triplas de números $p,\ p + 2$ y $p + 4$ tal que todas los tres números sean primos. Pruebe que se tienen todas dichas triplas.

22. Sea n entero. Muestre que exactamente una de las siguiente s afirmaciones se cumple $n = 4k$ para algún entero k, ó $n = 4k + 1$ para algún entero k, ó $n = 4k + 2$ para algún entero k, ó $n = 4k + 3$ para algún entero k. (Todo lo que se necesita es el hecho que todo entero es par ó impar.)

23. Sea n un entero impar. Muestre que existe un entero k tal que $n^2 = 8k + 1$.

24. Sea x un número real. Definimos el **valor absoluto** de x, denotado $|x|$, como

$$|x| = \begin{cases} x, & \text{if } x \geq 0, \\ -x, & \text{if } x < 0. \end{cases}$$

Sean x y y números reales. Pruebe las siguientes afirmaciones.

(i) $|-x| = |x|$.

(ii) $|x|^2 = x^2$.

(iii) $|x - y| = |y - x|$.

(iv) $|xy| = |x||y|$.

25. Sean x y y números reales. Definimos el $x \frown y$ y $x \smile y$ como

$$x \frown y = \begin{cases} x, & \text{if } x \geq y, \\ y, & \text{if } x \leq y. \end{cases} \qquad \text{y} \qquad x \smile y = \begin{cases} y, & \text{if } x \geq y, \\ x, & \text{if } x \leq y. \end{cases}$$

Sean $a,\ b$ y c números reales. Pruebe las siguientes afirmaciones.

(i) $(a \frown b) + (a \smile b) = a + b$.

(ii) $(a \smile b) + c = (a + c) \smile (b + c)$ y $(a \frown b) + c = (a + c) \frown (b + c)$.

(iii) $(a \frown b) \frown c = a \frown (b \frown c)$ y $(a \smile b) \smile c = a \smile (b \smile c)$.

(iv) $(a \frown b) - (a \smile b) = |a - b|$.

(v) $a \frown b = \frac{1}{2}(a + b + |a - b|)$ y $a \smile b = \frac{1}{2}(a + b - |a - b|)$

26. Sea x un número real. Denotamos por $\lfloor x \rfloor$ el mayor entero menor o igual que x. Para clarificar esta definición, note que existen únicos números I_x y $\sharp x$ tales que I_x es un entero, $0 \leq \sharp x < 1$ y $x = I_x + \sharp x$, entonces $\lfloor x \rfloor = I_x$. Sean x y y números reales. Pruebe las siguientes afirmaciones.

(i) $\lfloor x \rfloor + \lfloor -x \rfloor$ es igual a 0 ó -1.

(ii) $\lfloor x + y \rfloor$ es igual a $\lfloor x \rfloor + \lfloor y \rfloor$ ó $\lfloor x \rfloor + \lfloor y \rfloor + 1$

(iii) Si $x,\ y \geq 0$, entonces $\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor \leq \lfloor x \rfloor \lfloor y \rfloor + \lfloor x \rfloor + \lfloor y \rfloor$.

27. Pruebe ó dé un contraejemplo para cada una de las siguientes afirmaciones.

(i) Para cada número no negativo s, existe un número no negativo t tal que $s \geq t$.

(ii) Existe un número no negativo t tal que para todo número no negativo s, se tiene que $s \geq t$.

(iii) Para cada número no negativo t, existe un número no negativo s tal que $s \geq t$.

(iv) Existe un número no negativo s tal que para todo número no negativo t, se tiene que $s \geq t$.

28. Pruebe ó dé un contraejemplo para cada una de las siguientes afirmaciones.

(i) Para cada entero a, existe un entero b tal que $a|b$.

(ii) Existe un entero b tal que para todo entero a, se tiene que $a|b$

(iii) Para cada entero b, existe un entero a tal que $a|b$.

(iv) Existe un entero a tal que para todo entero b, se tiene que $a|b$.

29. Pruebe ó dé un contraejemplo para cada una de las siguientes afirmaciones.

(i) Para cada número real x, existe un número real y tal que $e^x - y > 0$.

(ii) Existe un número real y tal que para todo número real x, se tiene que $e^x - y > 0$

(iii) Para cada número real y, existe un número real x tal que $e^x - y > 0$.

(iv) Existe un número real x tal que para número real y, se tiene que $e^x - y > 0$.

30. Pruebe ó dé un contraejemplo para la siguiente afirmación: Para cada entero positivo a, existe un entero positivo b tal que
$$\frac{1}{2b^2 + b} < \frac{1}{ab^2}.$$

31. Pruebe ó dé un contraejemplo para la siguiente afirmación: Para todo número real y, existe un número real x tal que $e^{3x} + y = y^2 - 1$.

32. Pruebe ó dé un contraejemplo para la siguiente afirmación: Para cada entero x, y para cada entero y, existe un entero z tal que $z^2 + 2xz - y^2 = 0$.

33. Sea $P(x, y)$ una afirmación con variables libres x y y, las cuales son números reales. Sean a y b números reales. Decimos que el número real u es el mínimo $P-$número para a y b si las siguientes dos condiciones se satisfacen: (1) la afirmación $P(a, u)$ y $P(b, u)$ son verdaderas; (2) si w es un número real tal que $P(a, w)$ y $P(b, w)$ son verdaderas, entonces $u \leq w$. Suponga que c y d son números reales, y que existe un $P-$ número para c y d. Muestre que este mínimo $P-$número es único (un ejemplo familiar de esta situación es el mínimo común múltiplo).

Capítulo 3

Clases y Conjuntos.

La Teoría de Conjuntos es considerada la piedra angular de la matemática actual y a diferencia de la mayoría de los tópicos en matemáticas su creación fue obra de una sola persona, Georg Cantor en su artículo de 1874 llamado "On a Characteristic Property of All Real Algebraic Numbers". Es claro que el trabajo de Cantor fue influenciado por otros matemáticos tales como Richard Dedekind y algunos más antiguos como Zeno de Elea y Bernard Bolzano. No es de sorprender que el trabajo de Cantor no haya sido aceptado por los matemáticos de la época, debido a que el concepto de infinito no estaba bien entendido en ese momento. Desafortunadamente, en el momento en que la teoría de Cantor estaba siendo aceptada aparecieron la paradojas de las cuales las más famosa es la de Russel. Bertran Russel en 1901 demuestra que la teoría de conjuntos de Cantor era contradictoria, para eso definió el siguiente conjunto

$$S = \{a : a \notin a\}.$$

Entonces, si $S \in S$ se obtendría que $S \notin S$, lo cual es absurdo. De la misma forma, si $S \notin S$ se obtiene que $S \in S$, lo cual también es absurdo. Por tanto, se muestra que $S \in S$ si y sólo si $S \notin S$, la cual es una contradicción de las más fundamentales. Antes de las paradojas el asunto de la existencia de conjuntos no se había discutido. Más exactamente, Cantor y sus seguidores aceptaban el "sentido común" de que si podemos describir una propiedad de los objetos, también podemos hablar del conjunto de los objetos teniendo esa propiedad. La aparición de las paradojas marco el comienzo de una crisis de las bases de la matemática moderna, la cual no ha podido ser resuelta hasta el día de hoy. El primer intento por resolver los inconvenientes que generaron las paradojas fue hecho por Ernst Zermelo en 1908. Poco tiempo despúes Thoralf Skolem y Abraham Fraenkel refinaron el trabajo de Zermelo y obtienen la actual Teoría de Conjuntos aceptada por la mayoría de matemáticos del mundo. La existencia de las paradojas familiares fueron abolidas en la teoría de Zermelo-Fraenkel gracias al "Axioma de Selección" el cual dice lo siguiente: "Sean A un conjunto y $S(x)$ una afirmación acerca de x que tiene sentido para todo objeto x en A. Existe un conjunto el cual consiste en exactamente esos elementos x en A para los cuales se satisface $S(x)$". Note que con los axiomas de Zermelo-Fraenkel no se puede formar $\{x : x \notin x\}$, lo máximo que se puede hacer es crear $\{x \in A : x \notin x\}$, lo cual elimina la paradoja de Russell. En efecto, denote $S = \{x \in A : x \notin x\}$. En este caso es imposible que $S \in S$, pues si $S \in S$ se tendría que $S \notin S$, lo cual es una contradicción. Por tanto $S \notin S$. De lo que se sigue que $S \notin A$. Luego, el argumento de Russell meramente prueba

que si A es cualquier conjunto, entonces $\{x \in A : x \notin x\}$ no puede ser un elemento de A. Algunas variantes de la teoría de Zermelo-Fraenkel fueron creadas por John Von Neumann, Paul Bernays, Kurt Gödel, John Kelley y Anthony Morse. En la actualidad no estamos seguros que la teoría axiomática de conjuntos sea consistente, es decir, que este libre de contradicciones, lo que sabemos es que las contradicciones familiares, tales como la de Russel, no aparecen en las teorías de conjuntos actuales.

En este capítulo no haremos una teoría de conjuntos axiomática, todo lo contrario, será muy intuitiva, sólo queremos introducir las propiedades más importantes sobre conjuntos usadas en la matemática moderna y seguir practicando los métodos de demostración.

3.1. Definiciones Básicas.

Construiremos nuestra teoría estableciendo dos conceptos indefinibles: La palabra "clase" y la relación "pertenece a". Todos los objetos de nuestra teoría serán llamados clases. Ciertas clases que llamaremos conjuntos serán definidos más adelante. Todo conjunto es una clase, pero no el recíproco, esto es, no toda clase es una conjunto. Las clases que no son conjuntos serán llamadas clases propias. Por ejemplo, en la teoría axiomática de conjuntos la clase universal es propia.

Si x y A son clases la expresión "$x \in A$" se lee "x es un elemento de A", "x pertenece a A" o "x está en A". Es conveniente escribir "$x \notin A$" para decir que "x no es un elemento de A", "x no pertenece a A" o "x no está en A".

La manera más simple de representar clases es hacer una lista que encerramos entre llaves.

Ejemplo 3.1. *$\{a, b, c\}$ es la clase cuyos únicos elementos son a, b y c*

El orden de los elementos, no es importante. En la lista escribimos una única vez cada elemento. Puede haber clases infinitas y también las podemos representar como una lista entre llaves, la cual es seguida con puntos suspensivos. A continuación tenemos un ejemplo de esto.

Ejemplo 3.2. $\mathbb{N} = \{1, 2, 3, 4, ...\}$, $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.

A veces no los podemos listar y recurrimos a una propiedad, como se muestra a continuación.

Ejemplo 3.3. $P = \{m \in \mathbb{Z} : (\exists k \in \mathbb{Z})(m = 2k)\}$,
$P = \{m \in \mathbb{Z} : Existe\ un\ entero\ k\ tal\ que\ m = 2k\}$,
$P = \{x \in \mathbb{Z} : Existe\ un\ entero\ q\ tal\ que\ x = 2q\}$.

Observe que en las dos últimas definiciones lo único que cambia es la variable, pero las clases descritas son las mismas. Es decir el nombre de las variables es irrelevante.
La definición formal de intervalos de la recta real se hace por medio de propiedades.

Ejemplo 3.4. $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ *y* $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$

Nota 3.5. *Como el nombre de las variables es irrelevante, si uno se va a referir a un elemento de dicha clase hay que decirlo. Diríamos, por ejemplo: Sea $x \in (a,b)$... y mientras estamos en dicho contexto x tiene dicho sentido.*

Definición 3.6 (Igualdad de Clases)**.** *Sean A y B clases. Decimos que A es igual a B y lo denotamos por $A = B$, si cada elemento de A es un elemento de B y viceversa. En símbolos*

$$A = B \iff (\forall x)(x \in A \leftrightarrow x \in B).$$

Ejemplo 3.7. *Note que {a,b,c,d}={c,d,b,a}, es decir el orden como aparecen no es importante.*

Daremos ahora un ejemplo de como se muestra la igualdad de clases.

Ejemplo 3.8. *Sean $P = \{x \in \mathbb{R} : x^2 - 1 < 0\}$ y $Q = \{x \in \mathbb{R} : -1 < x < 1\}$ Probemos que $P = Q$.*

Prueba: Supongamos que $x \in P$, entonces $x^2 - 1 < 0$, luego $(x+1)(x-1) < 0$. Por tanto pueden ocurrir dos casos. Caso 1: $x - 1 < 0$ y $x + 1 > 0$. En este caso, $x < 1$ y $x > -1$, luego $-1 < x < 1$. Caso 2: $x - 1 > 0$ y $x + 1 < 0$, entonces $x < -1$ y $x > 1$, pero este caso es imposible. Luego el único caso que ocurre es el 1 y así $-1 < x < 1$, lo que implica $x \in Q$. Por tanto $x \in P \to x \in Q$.

Sea $x \in Q$, entonces $-1 < x < 1$, luego $-1 < x$ y $x < 1$. Así que $0 < x + 1$ y $x - 1 < 0$. Multiplicando tendremos que $(x-1)(x+1) < 0$, dado que tienen signos contrarios. Luego $x^2 - 1 < 0$ y así $x \in P$. Por tanto $x \in Q \to x \in P$. Lo que termina la prueba. □

Definición 3.9 (Subclases)**.** *Sean A y B clases. Decimos que A es una subclase de B "si $x \in A$, entonces $x \in B$". Esto lo denotamos por "$A \subseteq B$". En símbolos*

$$A \subseteq B \iff (\forall x)(x \in A \to x \in B).$$

Si A no es un subclase de B lo denotamos por "$A \not\subseteq B$". Escribiremos $A \subsetneq B$, para decir que $A \subseteq B$ pero que $A \neq B$.

Para probar que "$A \subseteq B$" la estrategia de la prueba es "Sea $x \in A$... argumentos, que generalmente involucran las definiciones de A y B... para concluir entonces $x \in B$, luego$A \subseteq B$". En cambio para probar que $A \not\subseteq B$ es suficiente exhibir un elemento que está en A y que no está en B. En efecto,

$$A \not\subseteq B \iff \sim [(\forall x)(x \in A \to x \in B)] \iff (\exists\, x)(x \in A \wedge x \notin B).$$

Ejemplo 3.10. *Sean $A = \{a,b\}, C = \{a,c,d,b\}$ y $D = \{c,d,a\}$. Nótese que $A \subseteq C, C \not\subseteq A, D \subseteq C, A \not\subseteq D, D \not\subseteq A$.*

Hacer una distinción entre los símbolos $\in$ y $\subseteq$ es muy importante. El ejemplo siguiente nos ayudará a clarificar el uso de los símbolos antes mencionados.

Ejemplo 3.11. *Las afirmaciones $a \in \{a,b,c\}$ y $\{a\} \subseteq \{a,b,c\}$ son proposiciones correctas, pero $\{a\} \in \{a,b,c\}$ y $a \subseteq \{a,b,c\}$ no lo son, pero sí podemos decir que $\{a\} \in \{\{a\},b,c\}$ aunque en este caso $\{a\} \subseteq \{\{a\},b,c\}$ es falso, pero sí es cierto que $\{\{a\}\} \subseteq \{\{a\},b,c\}$.*

Algunas propiedades básicas de la igualdad e inclusión de clases son dadas en el siguiente teorema.

Teorema 3.12. *Sean A, B y C clases. Entonces*

1. $A = A$
2. *Si* $A = B$, *entonces* $B = A$.
3. *Si* $A = B$ *y* $B = C$, *entonces* $A = C$.
4. $A \subseteq A$
5. $A \subseteq B$ *y* $B \subseteq A$ *si y sólo si* $A = B$.
6. *Si* $A \subseteq B$ *y* $B \subseteq C$, *entonces* $A \subseteq C$.

Prueba: Probaremos las primeras tres propiedades, el resto es dejado de ejercicio al lector.

1. Las afirmaciones $x \in A \to x \in A$ y $x \in A \to x \in A$ son claramente ciertas, entonces $A = A$.
2. Si $A = B$; entonces $x \in A \to x \in B$ y $x \in B \to x \in A$, entonces por la conmutativa del $\wedge$ se tiene que $x \in B \to x \in A$ y $x \in A \to x \in B$. Por definición de igualdad de clases, se tiene que $B = A$.
3. Supongamos que $A = B$ y $B = C$. Considere $x \in A$, entonces como $A = B$, se tiene que $x \in B$, pero $B = C$, luego $x \in C$. Así que la afirmación $x \in A \to x \in C$, es verdadera. De igual forma se prueba que $x \in C \to x \in A$ es válida, lo que muestra que $A = C$. □

Definición 3.13 (Clase vacío)**.** *La clase vacío es aquella que no tiene elementos, también se le llama algunas veces el clase nula y se denota por* $\varnothing$. *De forma axiomática se define como* $\varnothing = \{x : x \neq x\}$.

Definición 3.14 (Clase Universal o Universo)**.** *Definimos la clase universal o universo como la clase de todos los elementos, la denotaremos por U. De forma axiomática se define como*

$$U = \{x : x = x\}.$$

Lema 3.15. *Sea A una clase. Entonces* $\varnothing \subseteq A$ *y* $A \subseteq U$.

Prueba: (1) Como $a \in \varnothing$ es falso, ya que $\varnothing$ no tiene elementos, entonces "si $a \in \varnothing$ entonces $a \in A$" es verdadero, luego $\varnothing \subseteq A$.
(2) Si $x \in A$, entonces x es un elemento, luego $x \in U$. Por tanto $A \subseteq U$. □

3.2. Operaciones entre Clases.

Así como tenemos operaciones entre números, tenemos también operaciones entre clases. Las dos operaciones básicas corresponden al $\vee$ e $\wedge$ de la lógica.

Definición 3.16 (Unión e Intersección de Clases)**.** *Sean A y B clases. La unión de A y B, denotada por* $A \cup B$, *se define como la clase de todos los elementos que pertenecen a A o a B o a ambos A y B. En símbolos*

$$A \cup B = \{x : x \in A \ \vee \ x \in B\}.$$

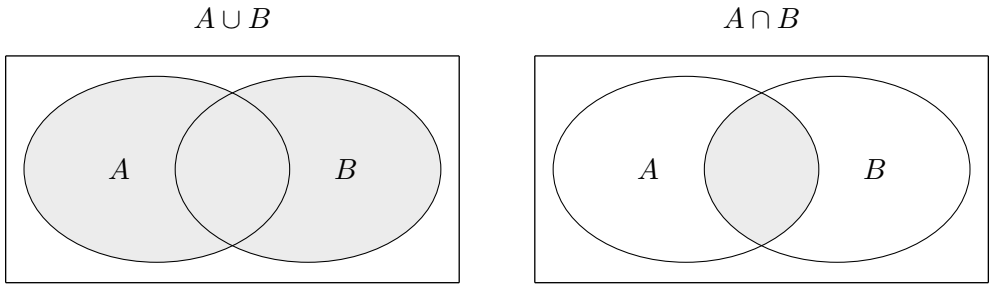
La intersección de A y B, denotada por $A \cap B$, *se define como la clase de todos los elementos que pertenecen a ambos A y B. En símbolos*

$$A \cap B = \{x : x \in A \ \wedge x \in B\}.$$

Ejemplo 3.17. *Sean* $A = \{1, 3, 5, -1\}$ *y* $B = \{-1, 0, 1\}$ *clases. Luego* $A \cup B = \{1, 3, 5, -1, 0\}$ *y* $A \cap B = \{-1, 1\}$.

Diagramas de Venn.

Son dibujos que nos ayudan a visualizar las clases, pero nunca reemplazan las pruebas aunque nos ayudan intuitivamente. A continuación se ilustra la unión e intersección de clases, las clases que queremos mostrar aparecen sombreadas.



Propiedades de la Unión e Intersección.

En el siguiente teorema tenemos las propiedades más importantes de la unión e intersección de clases.

Teorema 3.18. *Sean A, B y C clases.*

1. $A \cap B \subseteq A$ *y* $A \cap B \subseteq B$. *Si* X *es una clase tal que* $X \subseteq A$ *y* $X \subseteq B$ *entonces* $X \subseteq A \cap B$.
2. $A \subseteq A \cup B$ *y* $B \subseteq A \cup B$. *Si* Y *es una clase tal que* $A \subseteq Y$ *y* $B \subseteq Y$ *entonces* $A \cup B \subseteq Y$.
3. $A \cup B = B \cup A$ *y* $A \cap B = B \cap A$ *(Ley conmutativa).*
4. $A \cup (B \cup C) = (A \cup B) \cup C$ *y* $A \cap (B \cap C) = (A \cap B) \cap C$ *(Ley asociativa).*
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *y* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(Leyes distributivas).*
6. $A \cup \varnothing = A$ *y* $A \cap \varnothing = \varnothing$ *(Leyes modulativas o de identidad).*
7. $A \cup A = A$ *y* $A \cap A = A$ *(Leyes de idempotencia).*
8. $A \cup (A \cap B) = A$ *y* $A \cap (A \cup B) = A$ *(Leyes de absorción).*
9. *Si* $A \subseteq B$ *entonces* $A \cup C \subseteq B \cup C$ *y* $A \cap C \subseteq B \cap C$.

Prueba: Haremos algunas de las pruebas. Las otras son propuestas como ejercicio al lector.

1. Sean A y B clases, veamos que $A \cap B \subseteq A$. Sea $x \in A \cap B$, debemos concluir que $x \in A$. En efecto, si $x \in A \cap B$; entonces por definición de intersección $x \in A$ y $x \in B$. Usando

simplificación se tiene que $x \in A$, así pues $A \cap B \subseteq A$. De la misma forma se prueba que $A \cap B \subseteq B$.
Sea ahora X una clase tal que $X \subseteq A$ y $X \subseteq B$, veamos que $X \subseteq A \cap B$. Sea $x \in X$, como $X \subseteq A$ y $X \subseteq B$ se tiene que $x \in A$ y $x \in B$, luego por definición de intersección $x \in A \cap B$. Lo que muestra que $X \subseteq A \cap B$.

3. Como $x \in A$ o $x \in B$ es equivalente a $x \in B$ o $x \in A$ (por conmutatividad de la disyunción), entonces fácilmente se obtiene que $A \cup B = B \cup A$. Como ejercicio probar que $A \cap B = B \cap A$.

6. Sea $x \in A \cup \varnothing$ entonces $x \in A$ o $x \in \varnothing$. Pero como x no puede pertenecer al conjunto vacío, necesariamente $x \in A$ (aquí se esta usando que $P \vee CO \Leftrightarrow P$), luego $A \cup \varnothing \subseteq A$. Ahora, si $x \in A$ entonces por adición $x \in A$ o $x \in \varnothing$, luego $x \in A \cup \varnothing$, lo que implica $A \subseteq A \cup \varnothing$. Así se tiene que $A \cup \varnothing = A$.
Veamos ahora que $A \cap \varnothing = \varnothing$. Para eso tome $x \in A \cap \varnothing$, entonces $x \in A$ y $x \in \varnothing$. Por simplificación se tiene $x \in \varnothing$, lo que muestra que $A \cap \varnothing \subseteq \varnothing$. La otra contenencia es fácil de obtener del Lema 3.15(1), que en nuestro caso queda $\varnothing \subseteq A \cap \varnothing$. Lo que termina la prueba de este item. □

Definición 3.19 (Clases Disyuntas)**.** *Sean A y B clases. Decimos que A y B son disyuntas si no tienen elementos en común, es decir,*

$$A \cap B = \varnothing.$$

Ejemplo 3.20. *Sean $A = (2, 3)$ y $B = [3, 5)$ intervalos de la recta real. A y B son disyuntos.*

Definición 3.21 (Complemento de Clases)**.** *El complemento de una clase A, denotada por A', es la clase de todos los elementos que no pertenecen a A. En símbolos,*

$$A' = \{x : x \notin A\}.$$

Entonces $x \in A'$ si y sólo si $x \notin A$.

Teorema 3.22. *Sean A y B clases, entonces*

1. *$(A')' = A$ (Idempotencia).*
2. *$(A \cap B)' = A' \cup B'$ y $(A \cup B)' = A' \cap B'$ (Leyes de De Morgan).*

Prueba:

1. Por definición de complemento se tiene que

$$x \in (A')' \leftrightarrow x \notin A' \leftrightarrow x \in A.$$

Por tanto $(A')' = A$

2. Usando la definición de complemento y unión, se tiene que

$$x \in (A' \cup B') \leftrightarrow x \in A' \vee x \in B' \leftrightarrow x \notin A \vee x \notin B \leftrightarrow x \notin (A \cap B) \leftrightarrow x \in (A \cup B)'.$$

Por tanto $A' \cup B' = (A \cap B)'$. El resto de la prueba es dejada como ejercicio al lector.

Teorema 3.23. *Sea A una clase, entonces*

1. $A \cup U = U$
2. $A \cap U = A$
3. $U' = \varnothing$
4. $\varnothing' = U$
5. $A \cup A' = U$
6. $A \cap A' = \varnothing$

Prueba: Sólo haremos algunas de las pruebas el resto es dejado como ejercicio al lector.

1. Es claro que $A \cup U \subseteq U$, ya que U contiene a todas las clases. Considere $x \in U$, entonces por adición $x \in A \vee x \in U$, así que $x \in A \cup U$.
2. Claramente $\varnothing \subseteq U'$, pues vacío es subclase de cualquier clase, véase Lema 3.15(1). Sea $x \in U'$, entonces por definición de complemento se tiene que $x \notin U$, lo cual es absurdo, así que se puede concluir cualquier cosa, en particular $x \in \varnothing$. Por tanto $U' \subseteq \varnothing$.

Definición 3.24 (Diferencia de Clases)**.** *Sean A y B clases. La diferencia de A y B, denotada por $A - B$, es la clase definida por*

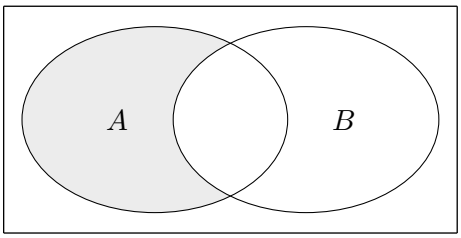
$$A - B = A \cap B'.$$

También se denota algunas veces por $A \setminus B$.

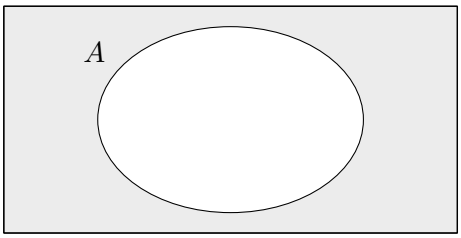
Ejemplo 3.25. *Si $A = \{x, y, z\}$ y $B = \{x, w\}$. Entonces $A - B = \{y, z\}$.*

A continuación se ilustra usando diagramas de Venn la diferencia y complemento de clases, las clases que queremos mostrar aparecen sombreadas.

$A - B$



A'



Propiedades de la Diferencia de Clases.

A continuación encontramos las propiedades más importantes de la diferencia de clases.

Teorema 3.26. *Sean A, B y C clases.*

1. $A - B \subseteq A \quad y \quad A - B \subseteq B'$.
2. $(A - B) \cap B = \varnothing$.
3. $A - B = \varnothing$ *si y sólo si* $A \subseteq B$.
4. $B - (B - A) = A$ *si y sólo si* $A \subseteq B$.
5. *Si* $A \subseteq B$, *entonces* $A - C = A \cap (B - C)$.
6. *Si* $A \subseteq B$, *entonces* $C - B \subseteq C - A$.

Prueba: Haremos algunas pruebas, las otras quedan como ejercicios.

2. Probemos que $(A-B)\cap B=\varnothing$. Ya sabemos que $\varnothing\subseteq(A-B)\cap B$, pues $\varnothing$ está contenido en cualquier clase. Sea $x\in(A-B)\cap B$, entonces $x\in(A-B)$ y $x\in B$, luego $x\in A$ y $x\notin B$ y $x\in B$, por simplificación se obtiene $x\in B$ y $x\notin B$, lo cual es una contradicción, luego la afirmación "Si $x\in(A-B)\cap B$, entonces $x\in\varnothing$" es cierta, pues el antecedente es falso. Luego $(A-B)\cap B\subseteq\varnothing$ y así obtenemos la igualdad buscada.

3. "$\Rightarrow$" Supongamos que $A-B=\varnothing$. Razonemos por contradicción, para esto suponga que $A\nsubseteq B$. Entonces existe un x_0 tal que $x_0\in A$ y $x_0\notin B$, luego $x_0\in A-B$, lo cual es absurdo, pues va en contra de la hipótesis de que $A-B=\varnothing$.
"$\Leftarrow$" Supongamos que $A\subseteq B$ y razonemos también por contradicción. Supongamos que $A-B\neq\varnothing$, luego existe un $x_0\in A-B$, es decir, $x_0\in A$ y $x_0\notin B$, pero como $A\subseteq B$ y $x_0\in A$, se obtiene que $x_0\in B$, lo cual es absurdo, pues tendríamos que $x_0\notin B$ y $x_0\in B$.

4. "$\Rightarrow$" Supongamos que $B-(B-A)=A$ y veamos que $A\subseteq B$. Sea $x\in A$, entonces $x\in B-(B-A)$, luego $x\in B$ y $x\notin(B-A)$ en particular $x\in B$. Luego $A\subseteq B$.
"$\Leftarrow$" Supongamos que $A\subseteq B$. Veamos que $B-(B-A)=A$.
"$\subseteq$" Sea $x\in B-(B-A)$ entonces $x\in B$ y $x\notin(B-A)$, pero negar que $x\in B-A$ es negar que $x\in B$ y $x\notin A$ y esto último es $x\notin B$ ó $x\in A$. Luego tenemos que $x\in B$ y ($x\notin B$ ó $x\in A$), lo cual es equivalente a ($x\in B$ y $x\notin B$) ó ($x\in B$ y $x\in A$). Como $x\in B$ y $x\notin B$ no puede ocurrir por ser una contradicción, entonces $x\in B$ y $x\in A$ ocurre, luego en particular $x\in A$. Así hemos probado que $B-(B-A)\subseteq A$.
"$\supseteq$" Sea ahora $x\in A$. Debemos probar que $x\in B-(B-A)$. Razonemos por contradicción, para eso supongamos que $x\notin B-(B-A)$, entonces $x\notin B$ o $x\in(B-A)$, así que tenemos dos casos. Caso 1: $x\notin B$, como $A\subseteq B$ y $x\in A$ entonces $x\in B$, lo cual es absurdo. Caso 2: $x\in(B-A)$. Así pues, $x\in B$ y $x\notin A$, luego por simplificación $x\notin A$. Pero esto es absurdo dado que $x\in A$. En cualquier caso se tiene un absurdo, lo que muestra que $x\in B-(B-A)$.

5. Supongamos que $A\subseteq B$. Veamos que $C-B\subseteq C-A$. Sea $x\in C-B$ entonces $x\in C$ y $x\notin B$, como $A\subseteq B$ entonces $x\notin A$, pues de lo contrario $x\in B$ y tendríamos una contradicción, luego $x\in C$ y $x\notin A$, es decir, $x\in C-A$. Por tanto $C-B\subseteq C-A$. □

3.3. Producto Cartesiano.

Definición 3.27 (Producto Cartesiano)**.** *Sean A y B clases. El producto (cartesiano) de A y B denotado por $A\times B$ es la clase*

$$A\times B=\{(a,b):a\in A\ y\ b\in B\},$$

donde (a,b) denota una pareja ordenada. La propiedad característica que define las parejas ordenadas es la siguiente:

$$(a,b)=(c,d)\quad si\ y\ sólo\ si\quad a=c\quad y\quad b=d.$$

Ejemplo 3.28. $A = \{a, b, c\}$ *y* $B = \{x, y\}$. $A \times B = \{(a, x), (a, y), (b, x), (b, y), (c, x), (c, y)\}$ *y* $B \times A = \{(x, a), (x, b), (x, c), (y, a), (y, b), (y, c)\}$. *Observemos que* $A \times B \neq B \times A$.

Ejemplo 3.29. *Al tirar un par de dados, uno primero que el otro, podemos obtener las siguientes parejas.*

	1	*2*	*3*	*4*	*5*	*6*
1	*(1,1)*	*(1,2)*	*(1,3)*	*(1,4)*	*(1,5)*	*(1,6)*
2	*(2,1)*	*(2,2)*	*(2,3)*	*(2,4)*	*(2,5)*	*(2,6)*
3	*(3,1)*	*(3,2)*	*(3,3)*	*(3,4)*	*(3,5)*	*(3,6)*
4	*(4,1)*	*(4,2)*	*(4,3)*	*(4,4)*	*(4,5)*	*(4,6)*
5	*(5,1)*	*(5,2)*	*(5,3)*	*(5,4)*	*(5,5)*	*(5,6)*
6	*(6,1)*	*(6,2)*	*(6,3)*	*(6,4)*	*(6,5)*	*(6,6)*

Se obtienen 36 elementos. En general es cierto que si A *tiene* n *elementos y* B *tiene* m *elementos, entonces* $A \times B$ *tiene* nm *elementos.*

Podemos definir productos con más de dos conjuntos así: $A \times B \times C = \{(a, b, c) : a \in A, b \in B$ y $c \in C\}$, donde (a, b, c) es una tripleta ordenada.

Ejemplo 3.30. $\mathbb{R}^3 = \{(x, y, z) : x \in \mathbb{R}, y \in \mathbb{R}$ *y* $z \in \mathbb{R}\}$.
$\mathbb{R} \times \mathbb{R} \cdots \times \mathbb{R} = \mathbb{R}^n = \{(x_1, x_2, ..., x_n) : \ x_i \in \mathbb{R}\}$.

Propiedades del Producto Cartesiano.

Teorema 3.31. *Sean A, B, C clases. Entonces*

1. *Si* $A \subseteq B$ *y* $C \subseteq D$, *entonces* $(A \times C) \subseteq (B \times D)$.
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$ *y* $(B \cup C) \times A = (B \times A) \cup (C \times A)$ *(Leyes distributivas).*
3. $A \times (B \cap C) = (A \times B) \cap (A \times C)$ *y* $(B \cap C) \times A = (B \times A) \cap (C \times A)$ *(Leyes distributivas).*
4. $A \times \varnothing = \varnothing$ *y* $\varnothing \times A = \varnothing$.
5. $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

Prueba: Probaremos sólo algunos de los numerales, los otros quedan como ejercicio al lector.

4. Veamos que $A \times \varnothing = \varnothing$. Ya sabemos que $\varnothing \subseteq A \times \varnothing$. Sea $x \in A \times \varnothing$ entonces $x = (a, b)$ con $a \in A$ y $b \in \varnothing$, pero como $b \in \varnothing$ es falso entonces $a \in A$ y $b \in \varnothing$ también lo es, luego $(a, b) \in \varnothing$ puesto que "Si $(a, b) \in A \times \varnothing$, entonces $(a, b) \in \varnothing$ " es verdadero ya que su antecedente es falso. Así $A \times \varnothing \subseteq \varnothing$ y entonces $A \times \varnothing = \varnothing$.

5. Veamos que $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.
"$\subseteq$" Sea $x \in (A \cap B) \times (C \cap D)$, entonces $x = (a, b)$ con $a \in A \cap B$ y $b \in C \cap D$. Luego $a \in A$ y $a \in B$ y $b \in C$ y $b \in D$, entonces $a \in A$ y $b \in C$ y $a \in B$ y $b \in D$. Así que $(a, b) \in A \times C$ y $(a, b) \in B \times D$, luego $x \in A \times C$ y $x \in B \times D$, lo que implica que $x \in (A \times C) \cap (B \times D)$. Hemos probado que $(A \cap B) \times (C \cap D) \subseteq (A \times C) \cap (B \times D)$. La otra contenencia queda como ejercicio al lector. □

Nota 3.32. *$(A \cup B) \times (C \cup D)$ no siempre es igual a $(A \times C) \cup (B \times D)$.*

Ejemplo 3.33. *Sean $A = \{a\}, B = C = \{b\}$ y $D = \{e, f\}$. Entonces*

$$A \cup B = \{a, b\}, \quad C \cup D = \{b, e, f\}, \; A \times C = \{(a, b)\}, B \times D = \{(b, c), (b, f)\},$$

$$(A \cup B) \times (C \cup D) = \{(a, b), (a, e), (a, f), (b, b), (b, e), (b, f)\} \quad y$$

$$(A \times C) \cup (B \times D) = \{(a, b), (b, e), (b, f)\}.$$

Note que $(A \cup B) \times (C \cup D) \not\subseteq (A \times C) \cup (B \times D)$.

3.4. Familias Indexadas de Clases.

Si tenemos tres conjuntos podemos describir su unión así $A \cup B \cup C = \{x : x \in A \text{ o } x \in B \text{ o } x \in C\}$. Pero si tenemos 50 conjuntos es difícil describir su unión o su intersección. Para esto usamos subíndices, por ejemplo $\{A_i\}_{i=1}^{50} = \{A_1, ..., A_{50}\}$. Además,

$$\bigcup_{i=1}^{50} A_i = \{x : x \in A_i, \text{ para algún } i \in \{1, \ldots, 50\}\}.$$

$$\bigcap_{i=1}^{50} A_i = \{x : x \in A_i, \text{ para todo } i \in \{1, \ldots, 50\}\}.$$

Si tenemos una clase A_i para cada $i \in \mathbb{N}$ entonces $\bigcup_{i=1}^{\infty} A_i = \{x : x \in A_i, \text{ para algún } i \in \mathbb{N}\}$ y $\bigcap_{i=1}^{\infty} A_i = \{x : x \in A_i, \text{ para todo } i \in \mathbb{N}\}$. Puede pasar que i no sea un número, sino simplemente una seña o una marca que lo diferencia de los otros. Así que si $I = \{\text{Todas las marcas}\}$, entonces $\bigcup_{i \in I} A_i = \{x : x \in A_i, \text{ para algún } i \in I\}$ y $\bigcap_{i \in I} A_i = \{x : x \in A_i, \text{ para todo } i \in I\}$.

Definición 3.34. *Sea I una clase no vacía. Supóngase que existe una clase denotada por A_i para cada $i \in I$. Tal colección de clases se llama una* **familia de clases** *indexada por I. La clase I es llamada la* **clase de índices**. *La unión y la intersección de todas las clases en la familia de clases están definidas por:*

$$\bigcup_{i \in I} A_i = \{x : x \in A_i, \quad \textit{para algún} \quad i \in I\}$$

y

$$\bigcap_{i \in I} A_i = \{x : x \in A_i, \quad \textit{para todo} \quad i \in I\}.$$

A continuación presentamos las propiedades más importantes de la unión e intersección de familias indexadas y luego haremos algunos ejemplos para fijar ideas.

Teorema 3.35. *Sea I una clase no vacía. Considere $\{A_i\}_{i\in I}$ una familia de clases indexada por I y B un clase cualquiera.*

1. $\bigcap_{i\in I} A_i \subseteq A_k$, *para todo* $k \in I$. *Si* $B \subseteq A_k$, *para todo* $k \in I$, *entonces* $B \subseteq \bigcap_{i\in I} A_i$.
2. $A_k \subseteq \bigcup_{i\in I} A_i$, *para todo* $k \in I$. *Si* $A_k \subseteq B$, *para todo* $k \in I$, *entonces* $\bigcup_{i\in I} A_i \subseteq B$.
3. $B \bigcap(\bigcup_{i\in I} A_i) = \bigcup_{i\in I}(B \bigcap A_i)$ *(Ley distributiva).*
4. $B \bigcup(\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(B \bigcup A_i)$ *(Ley distributiva).*
5. $(\bigcup_{i\in I} A_i)' = \bigcap_{i\in I} A_i'$ *(Ley de De Morgan).*
6. $(\bigcap_{i\in I} A_i)' = \bigcup_{i\in I} A_i'$ *(Ley de De Morgan).*

Prueba: Haremos algunas pruebas, las otras quedan como ejercicios al lector.

2. Veamos que para todo $k \in I, A_k \subseteq \bigcup_{i\in I} A_i$. Sea k_0 un elemento arbitrario de I. Tome $x \in A_{k_0}$, entonces $x \in A_{k_0}$, para algún k_0 en I, luego $x \in \bigcup_{i\in I} A_i$. Como k_0 es arbitrario en I, entonces para todo $k \in I$, se tiene que $A_k \subseteq \bigcup_{i\in I} A_i$.

4. Queremos probar la igualdad de conjuntos $B \cup (\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(B \cup Ai)$.
"$\subseteq$" Sea $x \in B \cup (\bigcap_{i\in I} A_i)$, entonces $x \in B$ ó $x \in \bigcap_{i\in I} A_i$. Razonemos por casos: Si $x \in B$, entonces $x \in B \cup A_i$ para todo $i \in I$, luego $x \in \bigcap_{i\in I}(B \cup Ai)$. Si $x \in \bigcap_{i\in I} A_i$ entonces $x \in A_i$ para todo $i \in I$, luego $x \in B \cup A_i$, para todo $i \in I$, pues $A_i \subseteq B \cup A_i$, para todo $i \in I$. Así que en este caso también $x \in \bigcap_{i\in I}(B \cup Ai)$.
"$\supseteq$" Sea $x \in \bigcap_{i\in I}(B \cup A_i)$, entonces $x \in B \cup A_i$, para todo $i \in I$. Hay dos casos posibles, que $x \in B$ ó que $x \notin B$. Si $x \in B$, entonces $x \in B \cup (\bigcap_{i\in I} Ai)$, pues $B \subseteq B \cup (\bigcap_{i\in I} Ai)$. Si $x \notin B$ entonces, como $x \in B \cup A_i$, para todo $i \in I$, necesariamente $x \in A_i$, para todo $i \in I$, luego $x \in \bigcap_{i\in I} A_i$. Y así $x \in B \cup (\bigcap_{i\in I} A_i)$, pues $\bigcap_{i\in I} A_i \subseteq B \cup (\bigcap_{i\in I} A_i)$.

5. Queremos probar que $(\bigcup_{i\in I} A_i)' = \bigcap_{i\in I} A_i'$
"$\subseteq$" Sea $x \in (\bigcup_{i\in I} A_i)'$, entonces $x \notin \bigcup_{i\in I} A_i$, luego para todo $i \in I$, $x \notin A_i$. De lo que se concluye que para todo $i \in I$ se tiene $x \in A_i'$. Por tanto $x \in \bigcap_{i\in I} A_i'$.
"$\supseteq$" Sea $x \in \bigcap_{i\in I} A_i'$, entonces $x \in A_i'$ para todo $i \in I$. Luego $x \notin A_i$ para todo $i \in I$, lo que implica que no existe $i \in I$ tal que $x \in A_i$ es decir $x \notin \bigcup_{i\in I} A_i$, así que $x \in (\bigcup_{i\in I} A_i)'$. □

Ejemplo 3.36. *Sean* $I = \mathbb{N}$ *y* $B_i = \{1, 2, ..., i\}$. *Entonces* $\bigcup_{i\in I} B_i = \mathbb{N}$ *y* $\bigcap_{i\in I} B_i = \{1\}$.
Prueba: *Veamos primero que* $\bigcup_{i\in I} B_i = \mathbb{N}$: *como* $B_i \subset \mathbb{N}$ *para todo* $i \in \mathbb{N}$, *por Teorema 3.35 (2) se tiene que* $\bigcup_{i\in I} B_i \subseteq \mathbb{N}$. *Para probar la otra contenencia considere* $n \in \mathbb{N}$. *Note que* $n \in B_n$ *y por definición de unión se concluye que* $n \in \bigcup_{i\in I} B_i$, *así que* $\mathbb{N} \subseteq \bigcup_{i\in I} B_i$. *Lo que termina la prueba de la primera igualdad.*
Veamos ahora que $\bigcap_{i\in I} B_i = \{1\}$: *como* $\{1\} \subset B_i$ *para todo* $i \in \mathbb{N}$ *por Teorema 3.35 (1) se tiene que* $\{1\} \subseteq \bigcap_{i\in I} B_i$. *La otra contenencia se obtiene fácilmente también del Teorema 3.35 (1), que en nuestro caso queda* $\bigcap_{i\in I} B_i \subseteq B_1 = \{1\}$. □

Para el siguiente ejemplo necesitaremos la Propeiedad Arquimediana de los Números Reales que dice así: Dado $\epsilon > 0$ y M un número real cualquiera, existe n un entero positivo tal que $n\epsilon > M$. Aceptaremos por ahora esta propiedad y la usaremos usualmente con $\epsilon = 1$.

Ejemplo 3.37. *Sea $I = \mathbb{N}$. Para cada $k \in \mathbb{N}$ definimos $F_k = \left(0, \frac{1}{k}\right)$. Entonces $\bigcup_{i\in I} F_i = (0,1)$ y $\bigcap_{i\in I} F_i = \varnothing$.*

Prueba: *Veamos primero que $\bigcup_{i\in I} F_i = (0,1)$: como $k \geq 1$ es claro que $F_k = (0, \frac{1}{k}) \subseteq (0,1)$, para todo $k \in \mathbb{N}$, por Teorema 3.35 (2) se tiene que $\bigcup_{i\in I} F_i \subseteq (0,1)$. Para probar la otra contenencia note que $(0,1) = F_1 \subseteq \bigcup_{i\in I} F_i$. Lo que termina la prueba de la primera igualdad.*
Veamos ahora que $\bigcap_{i\in I} F_i = \varnothing$. Claramente $\varnothing \subseteq \bigcap_{i\in I} F_i$, así que sólo debemos mostrar que $\bigcap_{i\in I} F_i \subseteq \varnothing$. para tal fin tome $x \in \bigcap_{i\in I} F_i$, por definición $x \in (0, \frac{1}{k})$ para todo $k \in \mathbb{N}$. Lo que implica que

$$0 < xk < 1 \quad \text{para todo} \quad k \in \mathbb{N}. \tag{3.1}$$

Aplicando la Propiedad Arquimediana debe existir $n \in \mathbb{N}$ tal que $nx > 1$, pero esto contradice (3.1), por tanto $x \in \varnothing$. □

Ejemplo 3.38. *Sea $I = (0, +\infty)$. Para cada $x \in (0, +\infty)$ sea $C_x = (-x, x)$ entonces $\bigcup_{x\in I} C_x = \mathbb{R}$ y $\bigcap_{x\in I} C_x = \{0\}$.*
Prueba: *Veamos primero que $\bigcup_{x\in I} C_x = \mathbb{R}$. Como $C_x \subset \mathbb{R}$ para todo $x \in I$, por Teorema 3.35 (2) se tiene que $\bigcup_{x\in I} C_x \subseteq \mathbb{R}$. Para probar la otra contenencia considere $y \in \mathbb{R}$. Note que $y \in C_{y+1}$ y por definición de unión se concluye que $y \in \bigcup_{x\in I} C_x$, así que $\mathbb{R} \subseteq \bigcup_{x\in I} C_x$. Lo que termina la prueba de la primera igualdad.*
Veamos ahora que $\bigcap_{x\in I} C_x = \{0\}$. Como $\{0\} \subset C_x$ para todo $x \in I$ por Teorema 3.35 (1) se tiene que $\{0\} \subseteq \bigcap_{x\in I} C_x$. Para la otra contenencia tome $y \in \bigcap_{x\in I} C_x$, por definición $y \in (-x, x)$ para todo $x \in I$. Lo que implica que

$$-x < y < x \quad \text{para todo} \quad x \in (0, +\infty). \tag{3.2}$$

Supongamos que $y \neq 0$, entonces tenemos dos casos $y > 0$ o $y < 0$. Si $y > 0$ aplicando la Propiedad Arquimediana existe $n \in \mathbb{N}$ tal que $ny > 1$, lo que implica $y > \frac{1}{n}$, pero esto contradice (3.2) si tomamos $x = \frac{1}{n}$. Si $y < 0$ aplicando de nuevo la Propiedad Arquimediana existe $m \in \mathbb{N}$ tal que $m(-y) > 1$, lo que implica $y < -\frac{1}{m}$, pero esto contradice (3.2) si tomamos $x = -\frac{1}{m}$, en cualquier caso tenemos un absurdo y por tanto $y = 0$, esto es $y \in \{0\}$. Lo que termina la prueba. □

Definición 3.39 (Conjunto)**.** *Entenderemos por conjunto cualquier clase que sea un elemento de una clase.*

Esta definición es basada en nuestra percepción intuitiva de lo que debe ser un conjunto. Si $A, B, C, ...$ son conjuntos, es perfectamente razonable que seamos capaces de formar una clase de la forma $\{A, B, C, ...\}$ cuyos elementos son $A, B, C, ...$ Es decir, ciertamente esperamos que cada conjunto sea un elemento. Lo contrario también es razonable, si A no es un conjunto, entonces A es una clase propia y para evitar contradicciones, las clases propias no deben ser elementos de nada. Luego, si A no es un conjunto, entonces A no debe ser un elemento.

A continuación enunciamos algunas propiedades de conjuntos sin dar una prueba.

Teorema 3.40. *(i) La clase vacía $\varnothing$ es un conjunto.*

(ii) Sea A un conjunto, el conjunto potencia $\mathscr{P}(A)$ (definido abajo) es un conjunto.

(iii) Sean A y B conjuntos, entonces $A \times B$ es un conjunto.

Definición 3.41 (Conjunto Potencia)**.** *Sea A un conjunto. El conjunto potencia de A, denotado $\mathscr{P}(A)$, es el conjunto cuyos elementos son todos los subconjuntos de A. Es decir*

$$\mathscr{P}(A) = \{X : X \subseteq A\}.$$

Ejemplo 3.42. *1. Sea $A = \{a, b, c\}$, luego $\mathscr{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}, \varnothing\}$.*

2. Para $\varnothing$ tenemos que $\mathscr{P}(\varnothing) = \{\varnothing\}$.

3. $\mathscr{P}(\mathscr{P}(\varnothing)) = \mathscr{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$

4. $\mathscr{P}(\mathscr{P}(\mathscr{P}(\varnothing))) = \mathscr{P}(\mathscr{P}(\{\varnothing\})) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$

Observación: $\varnothing \in \mathscr{P}(A)$ para todo A y lo mismo $A \in \mathscr{P}(A)$. En general es cierto que si un conjunto tiene n elementos, su conjunto potencia tiene 2^n elementos.

3.5. Ejercicios

1. Sean A, B, C clases. Muestre que si $A \subseteq B$, entonces $A \subseteq B \cup C$.
2. Encuentre conjuntos A y B tales que $A \in B$ y $A \subseteq B$.
3. Sean A y B clases, entonces
 (*i*) $A \subseteq B$ si y sólo si $A \cup B = B$,
 (*ii*) $A \subseteq B$ si y sólo si $A \cap B = A$.
4. Muestre que $A \cap (A' \cup B) = A \cap B$.
5. Muestre que $A - B = B' - A'$.
6. Sean $\{A_i\}_{i\in I}$ y $\{B_i\}_{i\in I}$ familias indexadas de clases. Muestre que
 (*i*) $\bigcup_{i\in I}(A_i \cap B_i) \subset \left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{i\in I} B_i\right)$,
 (*ii*) $\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{i\in I} A_i\right) \subset \bigcap_{i\in I}(A_i \cup B_i)$,
7. Sean $\{A_i\}_{i\in I}$ y $\{B_i\}_{i\in J}$ familias indexadas de clases. Muestre que
 (*i*) $\bigcup_{(i,j)\in I\times J}(A_i \cap B_j) = \left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right)$,
 (*ii*) $\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right) = \bigcap_{(i,j)\in I\times J}(A_i \cup B_j)$,
8. Sean A, B y C clases. Suponga que $A \subseteq B$, $B \subseteq C$ y $C \subseteq A$. Muestre que $A = B = C$.

9. Sean A y B clases cualesquiera. ¿Es cierto que una de las afirmaciones $A \subseteq B$ o $A = B$ o $B \subseteq A$ es verdadera? Dé una prueba o un contraejemplo.

10. Sea $A = \{x, y, z, w\}$. Liste todos lo elementos en $\mathscr{P}(A)$.

11. Sean A y B conjuntos. Suponga que $A \subseteq B$. Muestre que $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

12. Liste los elementos del conjunto $\mathscr{P}(\mathscr{P}(\{\varnothing\}))$.

13. Cuál de las siguientes afirmaciones es verdadera y cuál es falsa.

 (i) $\{\varnothing\} \subseteq G$ para todo conjunto G;
 (ii) $\varnothing \subseteq G$ para todo conjunto G;
 (iii) $\varnothing \subseteq \mathscr{P}(G)$ para todo conjunto G;
 (iv) $\{\varnothing\} \subseteq \mathscr{P}(G)$ para todo conjunto G;
 (v) $\varnothing \in G$ para todo conjunto G;
 (vi) $\varnothing \in \mathscr{P}(G)$ para todo conjunto G;
 (vii) $\{\{\varnothing\}\} \subseteq \mathscr{P}(\varnothing)$;
 (viii) $\{\varnothing\} \subseteq \{\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}\}$;
 (ix) $\mathscr{P}(\varnothing) = \{\varnothing, \{\varnothing\}\}$.

14. Considere dos clases A y B. ¿Son $A - B$ y $B - A$ clases necesariamente disjuntas? Dé una prueba o un contraejemplo.

15. Sea X una clase y asuma que $A, B, C \subseteq X$. Suponga que $A \cap B = A \cap C$ y $(X - A) \cap B = (X - A) \cap C$. Pruebe que $B = C$.

16. Sean A, B y C clases. Muestre que $(A - B) \cap C = (A \cap C) - B = (A \cap C) - (B \cap C)$.

17. Para números reales a, b y c sabemos que $a - (b - c) = (a - b) + c$. Descubra y pruebe una formula para $A - (B - C)$, donde A, B y C son clases.

18. Sea A y B clases. La **diferencia simétrica** de A y B, denotada $A \triangle B$, es la clase $A \triangle B = (A - B) \cup (B - A)$. Sean X, Y y Z clases. Muestre cada una de las siguientes afirmaciones.

 (i) $X \triangle \varnothing = X$.
 (ii) $X \triangle X = \varnothing$.
 (iii) $X \triangle Y = Y \triangle X$.
 (iv) $X \triangle (Y \triangle Z) = (X \triangle Y) \triangle Z$.
 (v) $X \cap (Y \triangle Z) = (X \cap Y) \triangle (X \cap Z)$.
 (vi) $X \triangle Y = (X \cup Y) - (X \cap Y)$.

19. Pruebe o encuentre un contraejemplo de la siguiente afirmación: Sean A, B y C clases. Entonces $(A - B) \cup C = (A \cup B \cup C) - (A \cap B)$.

20. Pruebe o encuentre un contraejemplo de la siguiente afirmación: Sean A, B y C clases. Entonces $(A \cup C) - B = (A - B) \cup (C - B)$.

21. Pruebe o encuentre un contraejemplo de la siguiente afirmación: Sean A, B y C clases. Entonces $(A \cup B) - (A \cap B \cap C) = [A - (B \cap C)] \cup [B - (A \cap C)$.

22. Sean A, B y C clases. Pruebe que $A \subseteq C$ si y sólo si $A \cup (B \cap C) = (A \cup B) \cap C$.

23. Pruebe o dé un contraejemplo para cada una de las siguientes afirmaciones.

 (i) Sean A, B y C conjuntos. Entonces $\mathscr{P}(A \cup B) = \mathscr{P}(A) \cup \mathscr{P}(B)$.

 (ii) Sean A, B y C conjuntos. Entonces $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$.

24. Muestre que no existen conjuntos A y B tales que $\mathscr{P}(A - B) = \mathscr{P}(A) - \mathscr{P}(B)$.

25. Sean A y B conjuntos. Muestre que

 (i) $A \subseteq B$ si y sólo si $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

 (ii) $A \cap B = \varnothing$ si y sólo si $\mathscr{P}(A) \cap \mathscr{P}(B) = \{\varnothing\}$.

26. Sean A, B y C clases. Pruebe que $A \times (B - C) = (A \times B) - (A \times C)$.

27. Sean A y B clases tales que $B \subseteq A$. Pruebe que

$$(A \times A) - (B \times B) = [(A - B) \times A] \cup [A \times (A - B)].$$

28. Sean A, B y E clases tales que $E \neq \varnothing$. Pruebe que si $A \times E = B \times E$, entonces $A = B$.

29. Sean A y B clases tales que $A \neq B$. Suponga que E es una clase tal que $A \times E = B \times E$. Pruebe que $E = \varnothing$.

30. Sean A y B clases no vacías. Muestre que $A = B$ si y sólo si $A \times B = B \times A$. ¿Qué pasa si $A = \varnothing$ o $B = \varnothing$?

31. Sean X un conjunto finito. ¿Cuál de los dos conjuntos $\mathscr{P}(X \times X) \times \mathscr{P}(X \times X)$ y $\mathscr{P}(\mathscr{P}(X))$ tiene mas elementos?

32. En cada uno de los siguientes casos, son dados conjuntos B_k para cada $k \in \mathbb{N}$, encuentre $\bigcup_{k\in\mathbb{N}} B_k$ y $\bigcap_{k\in\mathbb{N}} B_k$.

 (1) $B_k = \{0, 1, 2, 3, \ldots, 2k\}$ (2) $B_k = \{k - 1, k, k + 1\}$

 (3) $B_k = [\frac{3}{k}, \frac{5k+2}{k}) \cup \{10 + k\}$ (4) $B_k = [-1, 3 + \frac{1}{k}] \cup [5, \frac{5k+1}{k})$

 (5) $B_k = (-\frac{1}{k}, 1] \cup (2, \frac{3k-1}{k}]$ (6) $B_k = [0, \frac{k+1}{k+2}] \cup [7, \frac{7k+1}{k})$.

33. En cada uno de los siguientes casos, defina una familia de conjuntos $\{E_k\}_{k\in\mathbb{N}}$, donde $E_k \subseteq \mathbb{R}$ para cada $k \in \mathbb{N}$, los conjuntos E_k no son iguales, y satisfacen la propiedad dada.

 (i) $\bigcup_{k\in\mathbb{N}} E_k = [0, \infty)$ y $\bigcap_{k\in\mathbb{N}} E_k = [0, 1]$.

 (ii) $\bigcup_{k\in\mathbb{N}} E_k = (0, \infty)$ y $\bigcap_{k\in\mathbb{N}} E_k = \varnothing$.

 (iii) $\bigcup_{k\in\mathbb{N}} E_k = \mathbb{R}$ y $\bigcap_{k\in\mathbb{N}} E_k = \{3\}$.

 (iv) $\bigcup_{k\in\mathbb{N}} E_k = (2, 8)$ y $\bigcap_{k\in\mathbb{N}} E_k = [3, 6]$.

(v) $\bigcup_{k\in\mathbb{N}} E_k = (0,\infty)$ y $\bigcap_{k\in\mathbb{N}} E_k = \{1\}\cup[2,3)$.

(vi) $\bigcup_{k\in\mathbb{N}} E_k = \mathbb{Z}$ y $\bigcap_{k\in\mathbb{N}} E_k = \{...,-2,0,2,4,6,...\}$.

(vii) $\bigcup_{k\in\mathbb{N}} E_k = \mathbb{R}$ y $\bigcap_{k\in\mathbb{N}} E_k = \mathbb{N}$.

34. Sean I, J clases tales $J \subseteq I$ y $\{A_i\}_{i\in I}$ una familia de clases indexada por I.

(i) Muestre que $\bigcup_{j\in J} A_j \subseteq \bigcup_{i\in I} A_i$

(ii) Muestre que $\bigcap_{i\in I} A_i \subseteq \bigcap_{j\in J} A_j$

35. Sean I y B clases y $\{A_i\}_{i\in I}$ una familia de clases indexada por I.

(i) Muestre que $(\bigcup_{i\in I} A_i) - B = \bigcup_{i\in I}(A_i - B)$

(ii) Muestre que $(\bigcap_{i\in I} A_i) - B = \bigcap_{i\in I}(A_i - B)$

(iii) Muestre que $B \cup (\bigcup_{i\in I} A_i) = \bigcup_{i\in I}(B \cup A_i)$

(iv) Muestre que $B \cap (\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(B \cap A_i)$

(v) Muestre que $B \cap (\bigcup_{i\in I}(B \cup A_i)) = B$ y $B \cup (\bigcap_{i\in I}(B \cap A_i)) = B$.

36. Sean I una clase no vacía, B una clase y $\{A_i\}_{i\in I}$ una familia de clases indexada por I.

a) Muestre que $B \times (\bigcup_{i\in I} A_i) = \bigcup_{i\in I}(B \times A_i)$

b) Muestre que $B \times (\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(B \times A_i)$

37. Suponga que $\mathscr{W}$ es alguna propiedad de los subconjuntos de $\mathbb{R}$ (por ejemplo ser finito). Un subconjunto $X \subseteq \mathbb{R}$ es llamado co-$\mathscr{W}$ si $\mathbb{R} - X$ tiene la propiedad $\mathscr{W}$. Sea $\{X_i\}_{i\in I}$ una colección de subconjuntos co-$\mathscr{W}$ de $\mathbb{R}$, donde I es un conjunto de índices. Para cada una de las propiedades $\mathscr{W}$ listadas abajo, pruebe que $\bigcup_{i\in I} X_i$ es co-$\mathscr{W}$ ó de un contraejemplo. Trate de encontrar una regla general para decidir cuando $\bigcup_{i\in I} X_i$ es co-$\mathscr{W}$ para alguna propiedad $\mathscr{W}$ dada.

(i) Un subconjunto de $\mathbb{R}$ tiene la propiedad $\mathscr{W}$ si y sólo si este es finito.

(ii) Un subconjunto de $\mathbb{R}$ tiene la propiedad $\mathscr{W}$ si y sólo si este tiene a lo mas 7 elementos.

(iii) Un subconjunto de $\mathbb{R}$ tiene la propiedad $\mathscr{W}$ si y sólo si este tiene exactamente 7 elementos.

(iv) Un subconjunto de $\mathbb{R}$ tiene la propiedad $\mathscr{W}$ si y sólo si este contiene unicamente enteros.

(v) Un subconjunto de $\mathbb{R}$ tiene la propiedad $\mathscr{W}$ si y sólo si este es finito, y tiene un número par de elementos.

38. Sean I, J y L clases no vacías tales que $I = J \cup L$. Considere $\{A_i\}_{i\in I}$ una familia de clases indexada por I. Muestre que

(i) $\bigcup_{i\in I} A_j = \left(\bigcup_{i\in J} A_i\right) \cup \left(\bigcup_{i\in L} A_i\right)$.

(ii) $\bigcap_{i\in I} A_j = \left(\bigcap_{i\in J} A_i\right) \cap \left(\bigcap_{i\in L} A_i\right)$.

39. Sean I una clase no vacía y $\{A_i\}_{i\in I}$ una familia de clases indexada por I.

a) Si existe $k \in I$ tal que $A_k = \varnothing$, muestre que $\bigcup_{i\in I} A_i = \bigcup_{i\in J} A_i$, donde $J = I - \{k\}$, y $\bigcap_{i\in I} A_i = \varnothing$.

b) Si existe $k \in I$ tal que $A_k = U$, muestre que $\bigcup_{i\in I} A_i = U$ y $\bigcap_{i\in I} A_i = \bigcap_{i\in J} A_i$, donde $J = I - \{k\}$.

c) Si $A_i = A$ para todo $i \in I$, muestre que $\bigcup_{i\in I} A_i = A$ y $\bigcap_{i\in I} A_i = A$.

Capítulo 4

Funciones.

4.1. Funciones.

En este punto el lector ya debe haber tenido alguna experiencia en el manejo de funciones, desafortunadamente algunas veces se hace una introducción demasiado intuitiva y no queda claro en realidad lo que éstas son. En este capítulo intentamos llenar esos vacíos y dar las ideas fundamentales sobre funciones que serán útiles a otras áreas avanzadas de la Matemática. A pesar que las funciones son tan importantes, solamente en el siglo XIX los matemáticos comenzaron a examinar de forma detallada este concepto usando la lógica y no la intuición, lo que conocemos actualmente sobre funciones fue gracias a los trabajos de Gottlob Frege, Richard Dedekind, Giuseppe Peano, Bertrand Russell y Alfred Whitehead. A continuación formalizaremos la noción de función en términos de conjuntos.

Definición 4.1 (Función)**.** *Sean A y B conjuntos. Una función (también conocida como un mapeo) f de A en B, denotada por $f : A \to B$, es un subconjunto $F \subseteq A \times B$, tal que para todo $a \in A$ hay uno y sólo un par de la forma (a, b) en F. El conjunto A es llamado el dominio de la función f y el conjunto B es llamado el codominio de la función f.*

Así pues, una función consta de tres objetos:

- Un dominio A.
- Un codominio B.
- Un subconjunto F de $A \times B$ que cumple lo siguiente: (i) Para todo $x \in A$, existe $y \in B$ tal que $(x, y) \in F$. (ii) Si $(x, y_1) \in F$ y $(x, y_2) \in F$, entonces $y_1 = y_2$.

Ejemplo 4.2. *1. Consideremos los conjuntos $A = \{a, b, c, d\}, B = \{1, 2, 3, 4\}, D = \{1, 2, 3, 4, 5\}$. Sea $F \subset A \times B$, donde $F = \{(a, 2), (b, 1), (c, 4), (d, 4)\}$. F es una función con dominio A y codominio B. Si consideramos $F \subseteq A \times D$ resultan funciones diferentes, aunque la asignación es la misma, pues en este caso el codominio sería D y en el caso anterior es B.*

2. *Tenemos como regla de asignación $f(x) = \sqrt{x}$. ¿Es esto una función? Depende del dominio y el codominio. Si decimos que el dominio y el codominio son todos los reales, entonces no es una función. Debemos establecer el dominio y el codominio. Si tomamos como dominio $[0, +\infty)$ y codominio $\mathbb{R}$, entonces f es una función.*

Hemos definido funciones formalmente en términos de conjuntos, pero podemos recuperar la noción intuitiva de la regla de asignación. Trabajar con la noción formal de función, si bien nos garantiza la precisión de lo que digamos, es un poco engorroso y por tal motivo es más cómodo pensar en funciones en la forma como se hace en la mayoría de los libros. Lo que nos importa aquí es que dicha noción sí se puede formalizar. Observemos que lo que tenemos formalizado nos permite rescatar la regla de asignación. Sean $f : A \to B$ una función y $a \in A$, entonces existe un único par $(a, b) \in A \times B$ que pertence al conjunto $F \subseteq A \times B$, que define la función. Así podemos pensar que el par (a, b), está realmente asignándonos al elemento a un único elemento b de B. Notamos que el papel del conjunto F es el mismo que el de la regla de asignación. De todas formas es importante recordar que la regla de asignación sola no define la función. El dominio y el codominio deben ser claramente establecidos.

Definición 4.3. *Sean $f : A \to B$ una función y $a \in A$, entonces existe un único par $(a, b) \in F \subseteq A \times B$, que define la función. A este único elemento b, lo denotamos por $f(a)$ y decimos que es el valor de f en el elemento a o que es la imagen de a bajo f.*

Usos poco precisos de notación.

Es importante que estemos alertas con respecto a la notación, hay muchos libros elementales que son poco precisos en la notación. Muchas veces no dan explícitos ni el dominio ni el codominio. Veremos más adelante la importancia de distinguir estos conjuntos. Veamos algunos usos comunes e imprecisos de notación. Encontramos escrito: "sea $f(x)$ una función...", la imprecisión es que $f(x)$ no es la función, es la función evaluada en x. O encontramos escrito: "sea $f(x) = x^2 + 1$ una función", si bien entendemos más o menos lo que se quiere decir, nos queda la duda de cual sería el codominio. Quizás sería más preciso decir: "sea $f : \mathbb{R} \to \mathbb{R}$ una función, tal que $f(x) = x^2 + 1$, para todo $x \in \mathbb{R}$, o se podría decir: "sea $f : \mathbb{R} \to [1, \infty)$ una función tal que $f(x) = x^2 + 1$, para todo x en $\mathbb{R}$". Observamos que estas dos definiciones producen funciones diferentes, pues no coinciden en su codominio.

Nota 4.4. 1. *Cuantificar la variable al final es importante, pues esto nos dice que la regla de asignación es para todo x en $\mathbb{R}$.*

2. *Si bien, en cálculo sobreentendemos los dominios y suponemos el rango, para ser precisos debemos especificarlos. Por ejemplo "sea $f(x) = \sqrt{x}$ una función". Esto es incorrecto, debemos decir "sea $f : [0, \infty) \to \mathbb{R}$ una función tal que $f(x) = \sqrt{x}$, para todo $x \geq 0$".*

3. *Cuando definimos una función por tramos, y estos no son disyuntos, hay que verificar que las fórmulas coincidan en la intersección para garantizar que la fórmula esté bien definida. Veamos un ejemplo.*

$$|x| = \begin{cases} x, & si\ x \geq 0 \\ -x, & si\ x < 0 \end{cases}$$

no tiene problemas, pero si definimos

$$|x| = \begin{cases} x, & si\ x \geq 0 \\ -x, & si\ x \leq 0 \end{cases}$$

debemos verificar que $|0|$ *si esté bien definido, es decir, que no vaya a tomar dos valores diferentes. Note que en este caso no hay problema, pues* $|0| = 0 = -0$.

A continuación vemos que para que dos funciones sean iguales deben tener el mismo dominio, el mismo codominio y la misma regla de asignación.

Definición 4.5 (Igualdad de Funciones)**.** *Sean* f *y* g *funciones, decimos que* $f = g$ *si*

(*i*) f *y* g *tienen el mismo dominio, digamos* A

(*ii*) f *y* g *tienen el mismo codominio, digamos* B

(*iii*) *para todo* $x \in A$ *se tiene que* $f(x) = g(x)$.

Definición 4.6 (Funciones Particulares)**.** *Sean* A *y* B *conjuntos, y considere* $S \subseteq A$.

1. *Una función* **constante** $f : A \to B$ *es cualquier función para la cual* $f(x) = b$, *para todo* $x \in A$, *donde* b *es un elemento fijo de* B.
2. *La función* **identidad** *en* A *es la función* $1_A : A \to A$ *definida por* $1_A(x) = x$, *para todo* $x \in A$.
3. *La función* **inclusión** *de* S *en* A *es la función* $j : S \to A$ *definida por* $j(x) = x$, *para todo* $x \in S$.
4. *Si* $f : A \to B$ *es una función. La* **restricción** *de* f *a* S, *denotada por* $f|_S$, *es la función* $f|_S : S \to B$, *definida por* $f|_S(x) = f(x)$, *para todo* $x \in S$.
5. *Si* $g : S \to B$ *es una función, una* **extensión** *de* g *a* A *es cualquier función* $G : A \to B$, *tal que* $G|_S = g$.
6. *Las* **funciones proyecciones** *de* $A \times B$ *son las funciones* $\prod_1 : A \times B \to A$ *y* $\prod_2 : A \times B \to B$ *definidas por* $\prod_1((a, b)) = a$ *y* $\prod_2((a, b)) = b$, *para todo* $(a, b) \in A \times B$. *Similarmente tenemos* $\prod_i : A_1 \times ... \times A_i \times ... \times A_n \to A_i$ *es la función tal que* $\prod_i((a_1, a_2, ..., a_i, ..., a_n)) = a_i$, *para todo* $(a_1, a_2, ..., a_i, ..., a_n) \in A_1 \times ... \times A_i \times ... \times A_n$.

Veamos algunos ejemplos de funciones.

Ejemplo 4.7.

1. *Sean* $g : \mathbb{R}^+ \to \mathbb{R}$, *tal que* $g(x) = \sqrt{x}$, *para todo* $x \in \mathbb{R}^+$, *y* $G : \mathbb{R} \to \mathbb{R}$ *definida por* $G(x) = \begin{cases} -x, & si\ x \leq 0 \\ \sqrt{x}, & si\ x \geq 0 \end{cases}$, *entonces* G *es una extensión de* g *y* g *es una restricción de* G.
2. *Si* $S = \{x, y, z\}$ *y* $f : A \to A$ *está definida por* $f(x) = x, f(y) = y$ *y* $f(z) = z$, *entonces* $f = 1_A$.

3. *Si* $A = \{x, y, z\}$ *y* $B = \{a, b\}$, *entonces* $\prod_1 : A \times B \to A$ *es tal que* $\prod_1((x, a)) = x, \prod_1((x, b)) = x, \prod_1((y, a)) = y, \prod_1((y, b)) = y, \prod_1((z, a)) = z$ *y* $\prod_1((z, b)) = z$. *Además,* $\prod_2 : A \times B \to B$ *es tal que* $\prod_2((x, a)) = a, \prod_2((x, b)) = b$, *etc.*

4.2. Imagen e Imagen Inversa.

Supóngase que $N = \{x : x$ es un niño entre 7 y 14 años$\}$ y tenenos la función $f : N \to \mathbb{R}$ definida por $p(n)$ es el peso en kilogramos del niño n, para cada $n \in N$. Podemos preguntarnos por el conjunto de niños que pesan 43 kilos, este sería $\{n \in N : p(n) = 43\}$ o también por el conjunto de números que son el peso de algún niño entre 10 y 12 años $\{x : x = f(n)$, para algún n entre 10 y 12 años$\}$. Este estilo de conjuntos es muy común tener que calcularlos en el caso de cualquier función. Vamos a darles un nombre especial en la siguiente definición.

Definición 4.8 (Imagen e Imagen Inversa)**.** *Sea* $f : A \to B$ *una función.*

1. *Para cada* $P \subseteq A$, *sea* $f_*(P)$ *el conjunto definido por*

$$f_*(P) = \{b \in B : b = f(p), \quad \text{para algún} \quad p \in P\} = \{f(p) : p \in P\}.$$

 El conjunto $f_*(P)$ *se llama la imagen de* P *bajo* f.

2. *Para cada* $Q \subseteq B$, *sea* $f^*(Q)$ *definida por*

$$f^*(Q) = \{a \in A : f(a) = q, \quad \text{para algún} \quad q \in Q\} = \{a \in A : f(a) \in Q\}.$$

 El conjunto $f^*(Q)$ *se llama la imagen inversa o preimagen de* Q *bajo* f.

3. *El rango o imagen de* f, *denotado por* $\text{ran}f$, *se define como* $\text{ran}f = f_*(A)$.

Aunque la notaciones más usuales para $f_*(P)$ y $f^*(Q)$, son respectivamente $f(P)$ y $f^{-1}(Q)$, en este libro no las usaremos, pues si uno no tiene suficiente madurez matemática la notación usual podría hacernos incurrir en errores.

Ejemplo 4.9. *Sea* $f : \mathbb{R} \to \mathbb{R}$ *definida por* $f(x) = x^2 + 1$, *para todo* $x \in \mathbb{R}$. *Luego* $f_*((-1, 2]) = [1, 5]$, $f^*([1, 5]) = [-2, 2]$ *y* $f^*([0, \frac{1}{2})) = \varnothing$. *Observe que el codominio de* f *es* $\mathbb{R}$, *pero el rango es* $[1, +\infty)$. *Debemos tener cuidado de diferenciarlos bien.*

- *Vamos a probar que* $f_*((-1, 2]) = [1, 5]$. *Para esto tome* $y \in f_*((-1, 2])$, *entonces existe* $x \in (-1, 2]$ *tal que* $f(x) = y$, *esto es,* $x^2 + 1 = y$. *Como* $x \in (-1, 2]$ *tomaremos dos casos. Caso 1:* $-1 < x \leq 0$. *En este caso se tiene que* $0 \leq x^2 < 1$ *y por tanto* $1 \leq x^2 + 1 < 2$, *luego* $y \in [1, 2) \subseteq [1, 5]$. *Lo que muestra que* $f_*((-1, 2]) \subseteq [1, 5]$. *Caso 2:* $0 < x \leq 2$. *En este caso se tiene que* $0 < x^2 \leq 4$ *y así* $1 < x^2 + 1 \leq 5$, *por tanto* $y \in (1, 5] \subseteq [1, 5]$. *Luego* $f_*((-1, 2]) \subseteq [1, 5]$. *Veamos ahora la otra contenencia, esto es, que* $[1, 5] \subseteq f_*((-1, 2])$. *Para eso tome* $y \in [1, 5]$, *entonces* $0 \leq y - 1 \leq 4$, *tomando raíz cuadrada nos queda* $0 \leq \sqrt{y - 1} \leq 2$. *Por tanto si definimos* $x := \sqrt{y - 1}$, *se tiene que* $x \in [0, 2] \subseteq (-1, 2]$ *y es facil ver que* $f(x) = y$, *así que por definición de imagen se obtiene* $y \in f_*((-1, 2])$, *lo que muestra que* $f_*((-1, 2]) = [1, 5]$.

- *Veamos también que* $f^*([1,5]) = [-2,2]$. *En este caso se tiene* $x \in f^*([1,5])$ *si y sólo si* $f(x) \in [1,5]$ *si y sólo si* $1 \leq x^2+1 \leq 5$ *si y sólo si* $0 \leq x^2 \leq 4$ *si y sólo si* $-2 \leq x \leq 2$ *si y sólo si* $x \in [-2,2]$, *lo que muestra que* $f^*([1,5]) = [-2,2]$. *La prueba de que* $f^*([0,\frac{1}{2})) = \varnothing$ *es dejada como ejercicio al lector.*

Propiedades de las Imágenes e Imágenes Inversas.

Teorema 4.10. *Sea* $f : A \to B$ *una función. Considere* $C, D \subseteq A$ *y* $S, T \subseteq B$ *conjuntos. Sean* I *y* J *conjuntos no vacíos y considere* $\{U\}_{i\in I}$ *una familia de conjuntos indexada por* I *tal que* $U_i \subseteq A$, *para todo* $i \in I$, *y* $\{V\}_{j\in J}$ *una familia de conjuntos indexada por* J, *tal que* $V_j \subseteq B$, *para todo* $j \in J$. *Entonces:*

1. $f_*(\varnothing) = \varnothing$ *y* $f^*(\varnothing) = \varnothing$.
2. $f^*(B) = A$.
3. $f_*(C) \subseteq S$ *si y sólo si* $C \subseteq f^*(S)$.
4. *Si* $C \subseteq D$, *entonces* $f_*(C) \subseteq f_*(D)$
5. *Si* $S \subseteq T$, *entonces* $f^*(S) \subseteq f^*(T)$.
6. $f_*\left(\bigcup_{i\in I} U_i\right) = \bigcup_{i\in I} f_*(U_i)$.
7. $f_*\left(\bigcap_{i\in I} U_i\right) \subseteq \bigcap_{i\in I} f_*(U_i)$.
8. $f^*\left(\bigcup_{j\in J} V_j\right) = \bigcup_{j\in J} f^*(V_j)$.
9. $f^*\left(\bigcap_{j\in J} V_j\right) = \bigcap_{j\in J} f^*(V_j)$.

Prueba: Sólo haremos algunas pruebas, las restantes son dejadas como ejercicio al lector. Supongamos todas las hipótesis.

1. Veamos que $f_*(\varnothing) = \varnothing$. Sea $y \in f_*(\varnothing)$, luego existe $x \in \varnothing$ tal que $f(x) = y$. Pero esta afirmación es falsa, luego "si $y \in f_*(\varnothing)$, entonces $y \in \varnothing$" es verdadera, pues el antecedente es falso. Luego $f_*(\varnothing) \subseteq \varnothing$, pero como $\varnothing \subseteq f_*(\varnothing)$, pues $\varnothing$ es subconjunto de cualquier conjunto, entonces $f_*(\varnothing) = \varnothing$. Como ejercicio muestre que $f^*(\varnothing) = \varnothing$.

2. Veamos que $f^*(B) = A$. "$\subseteq$" Sea $x \in f^*(B)$, debemos probar que $x \in A$. En efecto, si $x \in f^*(B)$, entonces $x \in A$ y $f(x) \in B$ por definición de $f^*(B)$, luego en particular $x \in A$.
"$\supseteq$" Ahora si $x \in A$, como A es el dominio de f y B es el codominio, necesariamente $f(x) \in B$, luego $x \in f^*(B)$.

4. Supongamos que $C \subseteq D$ y probemos que $f_*(C) \subseteq f_*(D)$. Sea $y \in f_*(C)$, entonces existe $x \in C$ tal que $f(x) = y$ (por definición de f_*). Como $C \subseteq D$, entonces $x \in D$. Luego existe $x \in D$ tal que $f(x) = y$, así $y \in f_*(D)$ (por definición de f_*).

7. Probemos que $f_*(\bigcap_{i\in I} U_i) \subseteq \bigcap_{i\in I} f_*(U_i)$. Para esto tome $y \in f_*(\bigcap_{i\in I} U_i)$ entonces existe $x \in \bigcap_{i\in I} U_i$ tal que $f(x) = y$ (por definición de f_*), luego $x \in U_i$ para todo $i \in I$. Sea $k \in I$ arbitrario, entonces $x \in U_k$ y $f(x) = y$, luego $y \in f_*(U_k)$ y como k es arbitrario en I, se tiene que $y \in f_*(Ui)$, para todo $i \in I$, luego $y \in \bigcap_{i\in I} f_*(U_i)$.
Veamos con un contraejemplo que $\bigcap_{i\in I} f_*(U_i) \not\subseteq f_*(\bigcap_{i\in I} U_i)$. Consideremos $A = \{a, b, c, d\}, B = \{x, y, z\}$ y $f : A \to B$, tal que $f(a) = x$, $f(b) = f(c) = f(d) = y$. Sean $U_1 = \{a, b\}$ y $U_2 = \{c, d\}$, así $U_1 \cap U_2 = \varnothing, f_*(U_1 \cap U_2) = f_*(\varnothing) = \varnothing, f_*(U_1) = \{x, y\}, f_*(U_2) = \{y\}$ y $f_*(U_1) \cap f_*(U_2) = \{y\} \neq \varnothing$.

9. Veamos que $f^*(\bigcap_{j\in J} V_j) = \bigcap_{j\in J} f^*(V_j)$.
"$\subseteq$" Supongamos que $x \in f^*(\bigcap_{j\in J} V_j)$, entonces $f(x) \in \bigcap_{j\in J} V_j$ (por definición de f^*), luego $f(x) \in V_j$, para todo $j \in J$, lo que implica que $x \in f^*(V_j)$, para todo $j \in J$ (por definición de f^*), entonces $x \in \bigcap_{j\in J} f^*(V_j)$.

"$\supseteq$" Supongamos que $x \in \bigcap_{j\in J} f^*(V_j)$, entonces $x \in f^*(V_j)$, para todo $j \in J$, luego $f(x) \in V_j$, para todo $j \in J$, lo que implica que $f(x) \in \bigcap_{j\in J} V_j$ y así $x \in f^*(\bigcap_{j\in J} V_j)$. □

4.3. Composición de Funciones y Funciones Inversas.

Definición 4.11 (Composición). *Sean $f : A \to B$ y $g : B \to C$ funciones. La composición de f y g es la función $g \circ f : A \to C$ definida por $(g \circ f)(x) = g(f(x))$, para todo $x \in A$.*

Ejemplo 4.12. *Sean $f : [0, \infty) \to \mathbb{R}$, $g : \mathbb{R} \to [0, \infty)$, dadas por $f(x) = \sqrt{x}$ y $g(x) = x^2 + 1$ entonces $(g \circ f)(x) = g(f(x)) = \sqrt{x^2} + 1 = x + 1$ y $(f \circ g)(x) = f(g(x)) = \sqrt{x^2 + 1}$. Note que en este caso $f \circ g \neq g \circ f$.*

Propiedades de la Composición.

Lema 4.13. *Sean $f : A \to B$, $g : B \to C$ y $h : C \to D$ funciones. Entonces,*

1. *$(h \circ g) \circ f = h \circ (g \circ f)$ (Ley asociativa).*
2. *$f \circ 1_A = f$ y $1_B \circ f = f$ (Ley modulativa o de identidad).*

Prueba: 1. Veamos que $(h \circ g) \circ f = h \circ (g \circ f)$. Por la definición de la composición el dominio de $(h \circ g) \circ f$ y de $h \circ (g \circ f)$ es A y el codominio es D. Sea $x \in A$, mostremos que $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$. En efecto, $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$. Luego ambas funciones son iguales.

2. Recordemos que $1_A : A \to A$ es la función tal que $1_A(x) = x$, para todo $x \in A$. Veamos que $f \circ 1_A = f$. Primero que todo, observemos que ambas funciones tienen dominio A y codominio B. Considere $x \in A$, entonces $(f \circ 1_A)(x) = f(1_A(x)) = f(x)$ luego ambas funciones son iguales. Es dejado como ejercicio al lector mostrar que $1_B \circ f = f$, lo que termina le prueba. □

Definición 4.14 (Inversas a Derecha e Izquierda). *Sean $f : A \to B$ y $g : B \to A$ funciones.*

1. *La función g es una* **inversa a derecha** *para f si $f \circ g = 1_B$.*
2. *La función g es una* **inversa a izquierda** *para f si $g \circ f = 1_A$.*
3. *La función g es una* **inversa** *para f si lo es a derecha y a izquierda.*

Nota 4.15. *$f \circ g = 1_B$ quiere decir que $(f \circ g)(x) = 1_B(x) = x$, para todo $x \in B$ y $g \circ f = 1_A$ que quiere decir $(f \circ g)(x) = 1_A(x) = x$, para todo $x \in A$.*

Unicidad de las Funciones Inversas.

Lema 4.16. *Sea $f : A \to B$ una función.*

1. *Si f tiene una inversa, entonces esta inversa es única.*
2. *Si f tiene una inversa a derecha g y una inversa a izquierda h, entonces $g = h$ y por lo tanto, f tiene inversa.*
3. *Si f tiene inversa g, entonces g tiene inversa la cual es f.*

Prueba: 1. Supongamos que f tiene una función inversa g. Veamos que g es única, para lo cual supondremos que g' es otra inversa de f y probaremos que $g = g'$. Por definición de inversa, el dominio y el codominio de g y g' son iguales. Por hipótesis tenemos que $f \circ g = 1_B$, $g \circ f = 1_A$, $f \circ g' = 1_B$ y $g' \circ f = 1_A$. Entonces por el lema anterior tenemos que $g = 1_A \circ g = (g' \circ f) \circ g = g' \circ (f \circ g) = g' \circ 1_B = g'$, luego $g = g'$.

2. Como f tiene inversa a derecha g se tiene que $f \circ g = 1_B$ y como h es una inversa a izquierda de f obtenemos que $h \circ f = 1_A$. Usando estas dos últimas igualdades obtenemos que $g = 1_A \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ 1_B = h$. Por tanto $g = h$.

3. Como f tiene una inversa g entonces $f \circ g = 1_A$ y $g \circ f = 1_B$, luego $g \circ f = 1_B$ y $f \circ g = 1_A$ implican que g también tiene inversa y que ésta es justamente f. □

Definición 4.17 (Inversa). *Sea $f : A \to B$ una función. Si f tiene una inversa, entonces ésta se denota por f^{-1} y su dominio es B y codominio A.*

Nota 4.18. *Si una función tiene, por ejemplo, una inversa a derecha pero no a izquierda, ésta no tiene que ser única.*

Ejemplo 4.19. *Las siguientes funciones tienen inversa.*

1. *$f : \mathbb{R} \to \mathbb{R}$ tal que $f(x) = ax + b$, con $a \neq 0$ y para todo $x \in \mathbb{R}$.*
2. *$g : \mathbb{R} \to (0, \infty)$ tal que $g(x) = a^x$, con $a > 0, a \neq 1$ y para todo $x \in \mathbb{R}$.*
3. *$h : (0, \infty) \to \mathbb{R}$ tal que $h(x) = \log_a x$, para todo $x \in (0, \infty)$.*

4. *Sea $f : \mathbb{R} \to [0,\infty)$ tal que $f(x) = x^2$ para todo $x \in \mathbb{R}$. f no tiene inversa a izquierda pero si tiene diferentes inversas a derecha. En efecto, si $g : [0,\infty) \to \mathbb{R}$ es tal que $g(x) = \sqrt{x}$ entonces $(f \circ g)(x) = f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x$ para todo $x \in [0,\infty)$ y si $h : [0,\infty) \to \mathbb{R}$ es tal que $h(x) = -\sqrt{x}$, entonces $(f \circ h)(x) = f(h(x)) = f(-\sqrt{x}) = (-\sqrt{x})^2 = x$, para todo $x \in [0,\infty)$. Luego g y h son inversas a derecha de f. Para mostrar que f no tiene inversa a izquierda, razonemos por contradicción. Supongamos que f tiene una inversa $h : [0,\infty) \to \mathbb{R}$ a izquierda, luego $1_{\mathbb{R}} = h \circ f$. Entonces si $x \in \mathbb{R}$, se tiene que $1_{\mathbb{R}}(x) = x = (h \circ f)(x) = h(f(x)) = h(x^2)$, pero $1_{\mathbb{R}}(-x) = -x = (h \circ f)(-x) = h((-x)^2) = h(x^2)$, es decir, tendríamos que $x = -x$, para todo $x \in \mathbb{R}$, lo cual es absurdo. Luego f no puede tener una inversa a izquierda.*

5. *Sea $p : [0,\infty) \to \mathbb{R}$ definida por $p(x) = x^2$, para todo $x \in [0,\infty)$. Entonces p no tiene inversa a derecha, pero sí tiene diferentes inversas a izquierda. En efecto mostremos dos funciones que son inversas a izquierda para p. Sean $q, r : \mathbb{R} \to [0,\infty)$ definidas por*

$$q(x) = \begin{cases} \sqrt{x}, & si\ x \geq 0 \\ 1 - x, & si\ x < 0 \end{cases} \quad y \quad r(x) = \begin{cases} \sqrt{x}, & si\ x \geq 0 \\ 1 + 3x, & si\ x < 0 \end{cases}$$

Calculemos $q \circ p$ y $r \circ p$.

$$q \circ p(x) = q(p(x)) = q(x^2) = \sqrt{x^2} = x = 1_{[0,\infty)}(x), \quad si \quad x \geq 0,$$

$$r \circ p(x) = r(p(x)) = r(x^2) = \sqrt{x^2} = x = 1_{[0,\infty)}(x), \quad si \quad x \geq 0.$$

Vemos entonces que q y r son inversas a izquierda de p. Sin embargo, p no tiene inversa a derecha. En efecto, razonemos en este caso también por contradicción. Si p tuviera inversa a derecha, digamos g, entonces $p \circ g = 1_{\mathbb{R}}$ luego $1_{\mathbb{R}}(x) = x = p(g(x)) = (g(x))^2$, para todo $x \in \mathbb{R}$, pero esto es una contradicción si $x < 0$, ya que $(g(x))^2$ es positivo.

6. *Sea $s : \mathbb{R} \to \mathbb{R}$, definida por $s(x) = x^2$, para todo $x \in \mathbb{R}$, no tiene ni inversa a derecha ni inversa a izquierda. En efecto. Supongamos que $r : \mathbb{R} \to \mathbb{R}$ es una inversa a derecha para s. Entonces $s \circ r = 1_{\mathbb{R}}$. Luego $1_{\mathbb{R}}(x) = x = (s \circ r)(x) = s(r(x)) = (r(x))^2$, para todo $x \in \mathbb{R}$. Pero esto es un absurdo, pues $(r(x))^2$ siempre es positivo. Ahora supongamos que $h : \mathbb{R} \to \mathbb{R}$ es una inversa a izquierda para s. Entonces $(h \circ s)(x) = 1_{\mathbb{R}}(x)$, luego $1_{\mathbb{R}}(x) = x = (h \circ s)(x) = h(s(x)) = h(x^2)$, pero tambien $1_{\mathbb{R}}(-x) = -x = (h \circ s)(-x) = h(s(-x)) = h(x^2)$ luego $x = -x$ para todo $x \in \mathbb{R}$, lo cual es absurdo.*

4.4. Inyectividad, Sobreyectividad y Biyectividad.

Volvamos al ejemplo de las funciones $f : \mathbb{R} \longrightarrow [0,\infty)$ dada por $f(x) = x^2$, para todo $x \in \mathbb{R}$ y $p : [0,\infty) \longrightarrow \mathbb{R}$ dada por $p(x) = x^2$, para todo $x \in [0,\infty)$. Vimos que f no admite inversa a izquierda, porque si existiera h tal que $h \circ f = 1_{\mathbb{R}}$ encontraríamos que $x = (h \circ f)(x) = h(f(x)) = h(x^2) = h(f(-x)) = (h \circ f)(-x) = -x$. Entonces el obstáculo para encontrar la inversa a izquierda, es que hay dos elementos diferentes en el dominio de f que tienen la misma imagen. Por otro lado vimos que p no admite inversa a derecha porque si existiera g inversa a derecha tal que $p \circ g = 1_{\mathbb{R}}$ encontraríamos que $x = (p \circ g)(x) = p(g(x)) = (g(x))^2$, para todo $x \in \mathbb{R}$. Y el obstáculo aquí es

que $(g(x))^2 \geq 0$, esto es, que en el rango de p no tenemos valores negativos, luego el rango de p es distinto a su codominio. Estas dos clases de problemas son realmente los únicos obstáculos para que una función admita inversa a derecha o izquierda.

Definimos ahora funciones que no tienen esta clase de problemas.

Definición 4.20 (Inyectividad y Sobreyectividad)**.** *Sea $f : A \to B$ una función.*

1. *La función f es inyectiva (o uno a uno) si $x \neq y$ implica $f(x) \neq f(y)$, para todo $x, y \in A$. Equivalentemente (por contrarrecíproco) si $f(x) = f(y)$ implica $x = y$, para todo $x, y \in A$.*
2. *La función f es sobreyectiva (o sobre) si para todo $b \in B$, existe $a \in A$, tal que $f(a) = b$, equivalentemente $f_*(A) = B$.*
3. *La función f es biyectiva si es inyectiva y sobreyectiva.*

Ejemplo 4.21. *Veamos un ejemplo para cada definición.*

1. *$f : \mathbb{R} \to [0, \infty)$ dada por $f(x) = x^2$ no es inyectiva, pero sí es sobre.*
2. *$f : [0, \infty) \to \mathbb{R}$ dada por $f(x) = x^2$ es inyectiva, pero no es sobreyectiva.*
3. *$f : \mathbb{R} \to \mathbb{R}$ definida como $f(x) = x^2$ no es sobreyectiva y tampoco inyectiva.*
4. *$f : [0, \infty) \to [0, \infty)$, definida como $f(x) = x^2$ es biyectiva.*

Otra manera de pensar los conceptos anteriores es mirar cómo es $f^*(\{b\})$, para todo $b \in B$. Así, si $f : A \to B$ es una función, entonces:

(*i*) f es una función inyectiva si y sólo si para todo $b \in B$ se cumple que $f^*(\{b\})$ tiene a lo más un elemento (puede ocurrir que no tenga ninguno).

(*ii*) f es una función sobreyectiva si y sólo si para todo $b \in B, f^*(\{b\})$ tiene como mínimo un elemento (puede tener más de uno).

(*iii*) f es biyectiva si sólo si para todo $b \in B, f^*(\{b\})$ tiene exactamente un elemento.

Lema 4.22. *Sean $f : A \to B$ y $g : B \to C$ funciones.*

1. *Si f y g son ambas inyectivas, entonces $g \circ f$ también lo es.*
2. *Si f y g son ambas sobreyectivas, entonces $g \circ f$ también lo es.*
3. *Si f y g son ambas biyectivas, entonces $g \circ f$ también lo es.*

Prueba: 1. Supongamos que f y g son ambas funciones inyectivas. Para probar que $g \circ f$ también es inyectiva, probaremos que si $(g \circ f)(x) = (g \circ f)(y)$, entonces $x = y$, para todo $x, y \in A$. Supongamos que $(g \circ f)(x) = (g \circ f)(y)$, luego $g(f(x)) = g(f(y))$, y como g es inyectiva, entonces $f(x) = f(y)$, pero como f también es inyectiva, tendremos que $x = y$, para todo $x, y \in A$. Luego $g \circ f$ es inyectiva.

2. Supongamos que g y f son ambas funciones sobreyectivas. Para probar que $g \circ f$ es sobreyectiva, mostraremos que para todo $c \in C$, existe un $a \in A$ tal que $(g \circ f)(a) = c$. Sea c un elemento cualquiera de C. Como g es sobreyectiva, existe un $b \in B$ tal que $g(b) = c$, pero para este b, como f es sobreyectiva, entonces existe un $a \in A$ tal que $f(a) = b$, luego $g(b) = g(f(a)) = c$. Así, para cada $c \in C$ existe un $a \in A$ tal que $(g \circ f)(a) = c$. Luego $g \circ f$ es sobreyectiva.

3. Es consecuencia de 1 y 2. □

El recíproco de las afirmaciones 1, 2 y 3 no es necesariamente cierto. Veamos los siguientes ejemplos:

Ejemplo 4.23. *Considere $f : [0, \infty) \to \mathbb{R}$ dada por $f(x) = \sqrt{x}$ y $g : \mathbb{R} \to [0, \infty)$ definida como $g(x) = x^2$. Observamos que su composición $g \circ f : [0, \infty) \to [0, \infty)$, la cual es $(g \circ f)(x) = (\sqrt{x})^2 = x$ es sobreyectiva mientras que f no es sobre, aunque g sí lo es.*

El teorema que sigue responde nuestras preguntas del comienzo de la sección.

Teorema 4.24. *Sean A y B conjuntos no vacíos y $f : A \to B$ una función.*

1. *La función f tiene una inversa a derecha si y sólo si f es sobreyectiva.*
2. *La función f tiene una inversa a izquierda si y sólo si f es inyectiva.*
3. *La función f tiene inversa si y sólo si f es biyectiva.*

Prueba: Solo haremos una prueba, el resto es dejado como ejercicio al lector.

1. "⇒" Supongamos que f es una función que tiene una inversa a derecha $g : B \to A$. Veamos que f es sobreyectiva. Sea $b \in B$, entonces $g(b) \in A$ y si definimos $a = g(b)$ entonces $a \in A$ y $f(a) = f(g(b)) = (f \circ g)(b)$. Como g es inversa a derecha de f, tenemos que $f(a) = (f \circ g)(b) = 1_B(b) = b$, luego f es una función sobreyectiva.

 "⇐" Supongamos ahora que f es una función sobreyectiva. Veamos que existe una función $g : B \to A$ que es una inversa a derecha de f. Sea $b \in B$, entonces $f^*(\{b\})$ tiene al menos un elemento, pues f es sobreyectiva. Sea $a_b \in f^*(\{b\})$, luego $f(a_b) = b$. Entonces definamos $g : B \to A$ tal que $g(b) = a_b$ para todo $b \in B$. Por tanto $f(a_b) = f(g(b)) = (f \circ g)(b) = 1_B(b)$. Es decir g es una inversa a derecha de f. □

Nota 4.25. *En la prueba de la primera parte del Teorema 4.24, usamos* **el Axioma de Elección** *cuando escogemos un elemento a_b para cada conjunto $f^*(\{b\})$. El axioma de elección de manera un poco informal dice lo siguiente: Para cada familia de conjuntos no vacíos, existe otro conjunto que contiene un elemento de cada uno de ellos.*

Teorema 4.26. *Sean A y B conjuntos no vacíos y sea $f : A \to B$ una función.*

1. *La función f es sobreyectiva si y sólo si $g \circ f = h \circ f$ implica que $g = h$, para cualquier par de funciones $g, h : B \to X$, y para todo conjunto X.*
2. *La funcióon f es inyectiva si y sólo si $f \circ g = f \circ h$ implica que $g = h$, para cualquier par de funciones $g, h : Y \to A$, y para todo conjunto Y .*

Prueba: Sólo haremos la prueba de (2).

"$\Rightarrow$" Supongamos que f es inyectiva. Sean Y un conjunto cualquiera y $g, h : Y \to A$ dos funciones tales que $f \circ g = f \circ h$. Veamos que $g = h$. En efecto, sabemos que sus dominios y codominios coinciden, luego solo necesitamos mostrar que $g(y) = h(y)$ para todo $y \in Y$. Razonemos por contradicción, supongamos que existe $y \in Y$ tal que $g(y) \neq h(y)$, como f es inyectiva, entonces $f(g(y)) \neq f(h(y))$ pero esto contradice el hecho de que $f(g(y)) = f(h(y))$ para todo $y \in Y$. Luego necesariamente $g(y) = h(y)$, es decir $g = h$.
"$\Leftarrow$" Supongamos ahora que si $f \circ g = f \circ h$, entonces $g = h$, para todo par de funciones $g, h : Y \to A$ y todo conjunto Y . Probemos que f es inyectiva. Razonemos por reducción al absurdo. Supongamos que f no es inyectiva, entonces existen $a_1, a_2 \in A$, con $a_1 \neq a_2$ tales que $f(a_1) = f(a_2)$. Sean $Y = \{a_1, a_2\}$, $g : Y \to A$, tal que $g(a_1) = a_1$ y $g(a_2) = a_2$. Ademas considere $h : Y \to A$, definida como $h(a_1) = a_2$ y $h(a_2) = a_1$. Entonces $(f \circ g)(a_1) = f(g(a_1)) = f(a_1) = f(a_2) = f(h(a_1)) = (f \circ h)(a_1)$ y $(f \circ g)(a_2) = f(g(a_2)) = f(a_2) = f(a_1) = f(h(a_2)) = (f \circ h)(a_2)$. Luego $(f \circ g)(y) = (f \circ h)(y)$ para todo $y \in Y$, es decir $f \circ g = f \circ h$, pero esto contradice la hipótesis, pues claramente $g \neq h$. Luego f debe ser inyectiva. □

4.5. Ejercicios

1. ¿Cuál de las siguientes fórmulas define una función $\mathbb{R} \to \mathbb{R}$?

 (i) $f(x) = \operatorname{sen}(x)$ para todo $x \in \mathbb{R}$.

 (ii) $p(x) = \frac{x^2+3}{x+5}$ para todo $x \in \mathbb{R}$.

 (iii) $q(x) = \ln(x^4 + 1)$ para todo $x \in \mathbb{R}$.

 (iv) $r(x) = \begin{cases} e^x, & \text{si } x \geq 0 \\ \cos(x), & \text{si } x \leq 0. \end{cases}$

 (v) $s(x) = \begin{cases} x^2, & \text{si } x \geq 1 \\ x^3, & \text{si } x \leq 0. \end{cases}$

 (vi) $t(x) = \begin{cases} x^3 - 2, & \text{si } x \geq 1 \\ |x|, & \text{si } x \leq 1. \end{cases}$

 (vii) $g(x) = \begin{cases} \operatorname{sen}(x), & \text{si } x \geq \pi \\ x, & \text{si } x \leq \pi. \end{cases}$

2. Para cada una de las siguientes fórmulas encuentre el mayor conjunto $X \subseteq \mathbb{R}$ tal que $g : X \to \mathbb{R}$ es una función.

 (i) $g(x) = \frac{1}{x^4-3}$ para todo $x \in X$.

 (ii) $g(x) = \sqrt{1-x^2}$ para todo $x \in X$.

 (iii) $g(x) = 3\ln(\text{sen(x)})$ para todo $x \in X$.

 (iv) $g(x) = \begin{cases} \sqrt{x}, & \text{si } x \geq 0 \ \ y \ \ x \in X \\ x+1, & \text{si } x \leq 0 \ \ y \ \ x \in X. \end{cases}$

 (i) $g(x) = \begin{cases} \tan(\pi x) + 4, & \text{si } x \geq 1 \ \ y \ \ x \in X \\ 3x^2 + 1, & \text{si } x \leq 1 \ \ y \ \ x \in X. \end{cases}$

3. Sean A y B conjuntos, $S \subseteq A$ y $f : A \to B$ una función. Considere $g : A \to B$ una extensión de $f|_S$ a A. ¿Es $f = g$?

4. Sea X un conjunto. Para cada $A \subseteq X$ definimos la función característica $\mathscr{X}_A : X \to \{0,1\}$ como

$$\mathscr{X}_A(x) = \begin{cases} 1, & \text{si } x \in A \\ 0, & \text{si } x \in X - A. \end{cases}$$

 Sean $A, B \subseteq X$. Muestre que $\mathscr{X}_A = \mathscr{X}_B$ si y sólo si $A = B$.

5. Para cada una de las siguientes funciones $f : \mathbb{R} \to \mathbb{R}$ y cada $T \subset \mathbb{R}$ encuentre $f_*(T)$, $f^*(T)$, $f_*(f^*(T))$ y $f^*(f_*(T))$.

 (i) $f(x) = (x+1)^2$ para todo $x \in \mathbb{R}$ y $T = [-1, 1]$

 (ii) $f(x) = (x+1)^2$ para todo $x \in \mathbb{R}$ y $T = [-5, 2]$

 (iii) $f(x) = \lceil x \rceil$ para todo $x \in \mathbb{R}$, donde $\lceil x \rceil$ es el menor entero mayor o igual que x, y $T = (1, 3)$.

 (iv) $f(x) = \lfloor x \rfloor$ para todo $x \in \mathbb{R}$, donde $\lfloor x \rfloor$ es el mayor entero menor o igual que x, y $T = [0, 2] \cup (5, 7)$.

6. Sea $g : \mathbb{R}^2 \to \mathbb{R}$ dada por $g((x, y)) = xy$ para todo $(x, y) \in \mathbb{R}^2$. Haga un bosquejo de los siguientes conjuntos.

 (i) $g^*(\{3\})$.

 (ii) $g^*([-1, 1])$.

7. Sean X y Y conjuntos, $A \subseteq X$, $B \subseteq Y$ y considere $\pi_1 : X \times Y \to X$ y $\pi_2 : X \times Y \to Y$ las funciones proyección.

 (i) Muestre que $(\pi_1)^*(A) = A \times Y$ y $(\pi_2)^*(B) = X \times B$

 (ii) Muestre que $A \times B = (\pi_1)^*(A) \cap (\pi_2)^*(B)$

 (iii) Sea $P \subseteq X \times Y$. ¿Será que $P = (\pi_1)_*(P) \times (\pi_2)_*(P)$? Dé una prueba o un contraejemplo.

8. Encuentre la falla en el siguiente razonamiento de la prueba de la parte (viii) del Teorema 4.10, asumiendo que las partes (i)-(vii) han sido probadas: "Aplicando f_* a $f^*\left(\bigcup_{j\in J} V_j\right)$ obtenemos que $f_*\left(f^*\left(\bigcup_{j\in J} V_j\right)\right) = \bigcup_{j\in J} V_j$. Además, aplicando f_* a $\bigcup_{j\in J} f^*(V_j)$ y usando la parte (vi) del teorema, obtenemos que $f_*\left(\bigcup_{j\in J} f^*(V_j)\right) = \bigcup_{j\in J} f_*(f^*(V_j)) = \bigcup_{j\in J} V_j$. Como aplicando f_* a ambos lados de la ecuación en la parte (viii) tenemos el mismo resultado, concluimos que ésta es verdadera."

9. En este ejercicio mostramos que no es posible debilitar las afirmaciones en el Teorema 4.10 (iii).

 (i) Encuentre una función $f : A \to B$ junto con conjuntos $X \subseteq A$ y $Y \subseteq B$ tales que $f_*(X) = Y$ y $X \neq f^*(Y)$.

 (ii) Encuentre una función $g : J \to K$ junto con conjuntos $Z \subseteq J$ y $W \subseteq K$ tales que $f^*(W) = Z$ y $f_*(Z) \neq W$.

10. Encuentre un ejemplo que muestre que "$\subseteq$" en el Teorema 4.10 (vi) no puede ser remplazada por "$=$" (es suficiente usar la intersección de dos conjuntos).

11. (*i*) Encuentre una función $f : A \to B$ y subconjuntos $P, Q \subseteq A$ tales que $P \subsetneq Q$, pero que $f_*(P) = f_*(Q)$.

 (*ii*) Encuentre una función $g : C \to D$ y subconjuntos $S, T \subseteq D$ tales que $S \subsetneq T$, pero que $g^*(S) = g^*(T)$.

12. Sean $f : A \to B$ una funcióm y $P, Q \subseteq A$. Muestre que $f_*(P) - f_*(Q) \subseteq f_*(P - Q)$. ¿Necesariamente $f_*(P - Q) \subseteq f_*(P) - f_*(Q)$? Dé una prueba o un contraejemplo.

13. Sea $f : A \to B$ una función y $C, D \subseteq B$. Muestre que $f^*(D - C) = f^*(D) - f^*(C)$.

14. Sea $f : A \to B$ una función. Considere $X \subseteq A$ y $Y \subseteq B$.

 (i) Muestre que $X \subseteq f^*(f_*(X))$.

 (ii) Muestre que $f_*(f^*(Y)) \subseteq Y$.

 (iii) Muestre que $X = f^*(f_*(X))$ si y sólo si $X = f^*(Z)$ para algún $Z \subseteq B$.

 (iv) Muestre que $Y = f_*(f^*(Y))$ si y sólo si $Y = f_*(W)$ para algún $W \subseteq A$.

 (v) Muestre que $f_*(f^*(f_*(X))) = f_*(X)$.

 (vi) Muestre que $f^*(f_*(f^*(Y))) = f^*(Y)$.

15. Para cada una de las siguientes funciones $f : \mathbb{R} \to \mathbb{R}$, encuentre funciones diferentes de la identidad $g, h : \mathbb{R} \to \mathbb{R}$ tales que $f = h \circ g$.

 (i) $f(x) = \sqrt{x+7}$ para todo $x \geq -7$.

 (ii) $f(x) = \sqrt{x} + 7$ para todo $x \geq 0$.

 (iii) $f(x) = \begin{cases} x^6, & \text{si } x \geq 0 \\ x^4, & \text{si } x < 0. \end{cases}$

(iv) $f(x) = \begin{cases} x^3, & \text{si } x \geq 0 \\ x, & \text{si } x < 0. \end{cases}$

16. Sean $f, g : \mathbb{R} \to \mathbb{R}$ dadas por

$$f(x) = \begin{cases} 1 - 2x, & \text{si } x \geq 0 \\ |x|, & \text{si } x < 0. \end{cases} \qquad g(x) = \begin{cases} 3x, & \text{si } x \geq 0 \\ x - 1, & \text{si } x < 0. \end{cases}$$

Encuentre $f \circ g$ y $g \circ f$.

17. (*i*) Encuentre funciones $h, k : \mathbb{R} \to \mathbb{R}$ tales que tanto h como k no sean constantes y sin embargo $k \circ h$ sea constante.

(*i*) Encuentre funciones $s, t : \mathbb{R} \to \mathbb{R}$ tales que $s \neq 1_{\mathbb{R}}$ y $t \neq 1_{\mathbb{R}}$, pero que $t \circ s = 1_{\mathbb{R}}$

18. Sean $f : A \to B$ y $g : B \to C$ funciones, $U \subseteq A$ y $V \subseteq C$ subconjuntos. Muestre que

$$(g \circ f)_*(U) = g_*(f_*(U)) \qquad \text{y} \qquad (g \circ f)^*(V) = f^*(g^*(V)).$$

19. Sean $f : A \to B$ y $g : B \to C$ funciones tales que ambas tienen inversa. Muestre que $g \circ f$ tiene inversa y que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

20. Encuentre dos inversas a derecha para cada una de las siguientes funciones

(i) Sea $f : \mathbb{R} \to [0, \infty)$ dada por $f(x) = |x|$ para todo $x \in \mathbb{R}$.

(ii) Sea $g : \mathbb{R} \to [1, \infty)$ dada por $g(x) = e^{x^2}$ para todo $x \in \mathbb{R}$.

21. Encuentre dos inversas a izquierda para cada una de las siguientes funciones

(i) Sea $f : [0, \infty) \to \mathbb{R}$ dada por $f(x) = x^3 + 4$ para todo $x \in [0, \infty)$.

(ii) Sea $g : \mathbb{R} \to \mathbb{R}$ dada por $g(x) = e^x$ para todo $x \in \mathbb{R}$.

22. Defina las funciones $h, k : \mathbb{R} \to \mathbb{R}$ por

$$h(x) = \begin{cases} 4x + 1, & \text{si } x \geq 0 \\ x, & \text{si } x < 0. \end{cases} \qquad k(x) = \begin{cases} 3x, & \text{si } x \geq 0 \\ x + 3, & \text{si } x < 0. \end{cases}$$

Encuentre una inversa para $k \circ h$.

23. Sea $f : A \to B$ una función. Muestre que si f tiene dos inversas distintas a izquierda, entonces no tiene inversa a derecha. Muestre que si f tiene dos inversas distintas a derecha, entonces no tiene inversa a izquierda.

24. Sean $A, A_1, ..., A_k$ conjuntos para algún entero positivo k. Considere $f : A \to A_1 \cdots \times A_k$ y $U_i \subseteq A_i$ para todo $i \in \{1, 2, ..., k\}$. Muestre que

$$f^*(U_1 \times \cdots \times U_k) = \bigcap_{i=1}^{k} (f_i)^*(U_i),$$

donde las f_i son las coordenadas de la función f.

25. Sean $A, A_1, ..., A_k$ conjuntos para algún entero positivo k y $h_i : A \to A_i$ una función para cada $i \in \{1, 2, ..., k\}$. Muestre que existe una única función $g : A \to A_1 \times \cdots \times A_k$ tal que $\pi_i \circ g = h_i$ para todo $i \in \{1, 2, ..., k\}$, donde $\pi_i : A_1 \times \cdots \times A_k \to A_i$ es la función proyección.

26. Sean A y B conjuntos, y considere $S \subseteq A$.

 (i) Muestre que la función identidad $1_A : A \to A$ es biyectiva.

 (ii) Muestre que la función inclusión $j : S \to A$ es inyectiva.

 (iii) Suponga que $f : A \to B$ es una función inyectiva. ¿Es la restricción $f|_S$ necesariamente inyectiva? Pruébelo o dé un contraejemplo.

 (iv) Suponga que $g : A \to B$ es una función sobreyectiva. ¿Es la restricción $g|_S$ necesariamente sobreyectiva? Pruébelo o dé un contraejemplo.

 (v) Suponga que $h : S \to B$ es una función inyectiva y considere $H : A \to B$ la extensión de h. ¿Es H necesariamente inyectiva? Pruébelo o dé un contraejemplo.

 (vi) Suponga que $k : S \to B$ es una función sobreyectiva, y considere $K : A \to B$ la extensión de k. ¿Es K necesariamente sobreyectiva? Pruébelo o dé un contraejemplo.

 (vii) Muestre que las funciones proyecciones $\pi_1 : A \times B \to A$ y $\pi_2 : A \times B \to B$ son sobreyectivas. ¿Son estas funciones proyección inyectivas?

27. Sean h y k como en el Ejercicio 22. ¿Es $h \circ k$ biyectiva, inyectiva, sobre o ninguna de las anteriores?

28. Sean A y B conjuntos. Muestre que existe una función biyectiva $f : A \times B \to B \times A$.

29. Sean A, B y C conjuntos. Muestre que existe una función biyectiva $g : (A \times B) \times C \to A \times (B \times C)$.

30. Sea A un conjunto. Defina $\phi : \mathscr{P}(A) \to \mathscr{P}(A)$ por $\phi(X) = A - X$, para todo $X \in \mathscr{P}(A)$. Muestre que ϕ es biyectiva.

31. Defina $\mathbb{L}$ de la siguiente forma:

$$\mathbb{L} = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a \text{ y } b \text{ son primos relativos.}\}$$

 Defina dos funciones $U, D : \mathbb{L} \to \mathbb{L}$ por $U(a, b) = (a + b, b)$ y $D(a, b) = (a, a + b)$, para todo $(a, b) \in \mathbb{L}$.

 (i) Muestre $(1, 1) \notin U(\mathbb{L})$ y $(1, 1) \notin D(\mathbb{L})$.

 (ii) Mustre $U((a, b)) \neq (a, b)$ y $D((a, b)) \neq (a, b)$ para todo $(a, b) \in \mathbb{L}$.

 (iii) Muestre U y D son ambas inyectivas.

 (iv) Muestre $U(\mathbb{L}) \cap D(\mathbb{L}) = \varnothing$.

32. Sean $f : A \to B$ una función inyectiva y $P, Q \subseteq A$. Muestre $f_*(P - Q) = f_*(P) - f_*(Q)$.

33. Sea $f : A \to B$ una función.

 (i) Muestre f es inyectiva si y sólo si $E = f^*(f_*(E))$, para todos los subconjuntos $E \subseteq A$.

(ii) Muestre f es sobreyectiva si y sólo si $F = f_*(f^*(F))$, para todos los subconjuntos $F \subseteq B$.

34. Sean $f : A \to B$ y $g : B \to A$ funciones.

(i) Suponga que f es sobreyectiva, y que g es una inversa a derecha de f. Muestre que g es inyectiva.

(ii) Suponga que f es inyectiva, y que g es una inversa a izquierda de f. Muestre que g es sobreyectiva.

(iii) Suponga que f es biyectiva, y que g es la inversa de f. Muestre que g es biyectiva.

35. Sean $f : A \to B$ y $g : B \to C$ funciones.

(i) Muestre que si $g \circ f$ es inyectiva, entonces f es inyectiva.

(ii) Muestre que si $g \circ f$ es sobreyectiva, entonces g es sobreyectiva.

(iii) Muestre que si $g \circ f$ es biyectiva, entonces f es inyectiva y g es sobreyectiva.

(iv) Encuentre un ejemplo de funciones $f : A \to B$ y $g : B \to C$ tales que $g \circ f$ sea biyectiva, pero f no es sobreyectiva y g no es inyectiva.

36. Sea $f : A \to B$ una función. Muestre que f es sobreyectiva si y sólo si $B - f_*(X) \subseteq f_*(A - X)$, para todo $X \subseteq A$.

37. Sea $h : X \to Y$ una función. Muestre que h es inyectiva si y sólo si $h_*(A \cap B) = h_*(A) \cap h_*(B)$, para todo $A, B \subseteq X$.

38. Sea $f : A \to B$ una función. Defina $F : \mathscr{P}(A) \to \mathscr{P}(B)$ como $F(X) = f_*(X)$, para todo $X \subseteq A$ y $G : \mathscr{P}(B) \to \mathscr{P}(A)$ como $G(Y) = f^*(Y)$, para todo $Y \subseteq B$.

(i) Muestre que F es sobreyectiva si y sólo si f es sobreyectiva.

(ii) Muestre que F es inyectiva si y sólo si f es inyectiva.

(iii) Muestre que G es sobreyectiva si y sólo si f es inyectiva.

(iv) Muestre que G es inyectiva si y sólo si f es sobreyectiva.

(v) Muestre que F es biyectiva si y sólo si G es biyectiva si y sólo si f es biyectiva.

(vi) Suponga que f es biyectiva. Muestre que F y G son inversas una de la otra.

39. Sean $f : A \to B$ una función, $D \subseteq A$ y $T \subseteq B$.

(i) Muestre que no siempre se tiene que $f^*(T) \subseteq D$, implica $T \subseteq f_*(D)$

(ii) Muestre que si f es sobreyectiva, entonces se tiene que $f^*(T) \subseteq D$, implica $T \subseteq f_*(D)$.

Capítulo 5

Relaciones.

5.1. Conceptos Fundamentales.

La teoría sobre relaciones es fundamental en las bases de la Matemática, a pesar de que Aristóteles mencionaba la palabra relación y los matemáticos medievales hablaron de manera más extensa sobre éstas, solamente en el siglo XIX Bertrand Rusell y Alfred Whitehead definen de manera precisa lo que es una relación y lo hacen en su famoso trabajo "Principia Mathematica". En el lenguaje común decimos que hay una relación entre dos cosas si existe alguna conexión entre ellas. Por ejemplo, podemos pensar que las personas estén relacionadas si ellas tienen el mismo color de ojos o el mismo color de cabello. En matemáticas a veces relacionamos también objetos, por ejemplo, entre números tenemos las relaciones $<$ ó $\leq$ ó $=$; o entre conjuntos las relaciones $\subset$ ó $\subseteq$ ó $=$. En este capítulo estudiaremos las ideas básicas sobre relaciones y después definiremos un tipo de relación muy especial que llamaremos de equivalencia.

De manera similar a las funciones, definimos relaciones como conjuntos de parejas ordenadas.

Definición 5.1 (Relación)**.** *Sean A y B conjuntos. Decimos que R es una relación de A en B si R es un subconjunto $A \times B$. Si $a \in A$ y $b \in B$, decimos que a está relacionado con b, lo cual denotamos por aRb, si $(a, b) \in R$. La notación $a\not{R}b$ significa que a no está relacionado con b. Una relación de A en A es llamada simplemente una relación en A.*

Ejemplo 5.2.

1. *Sean $A = \{a, b\}, B = \{x, y, z\}$. Podemos definir la siguiente relación, $R = \{(a, x), (a, y), (b, z)\}$, note que aRx, aRy y bRz.*

2. *Los símbolos $<$, $\leq$, $=$ representan relaciones entre números reales.*

3. *Los símbolos $\subset$, $\subseteq$, $=$ representan relaciones entre conjuntos.*

4. *Dada cualquier función $f : A \to B$ representa una relación donde aRb si y sólo si $f(a) = b$.*

5. *En $\mathbb{Z}$ tenemos, por ejemplo, la relación x divide a y, es decir, xRy si y sólo si $x|y$.*

Definición 5.3 (Clases). *Sean A y B conjuntos no vacíos, y R una relación de A en B. Para cada $x \in A$ definimos la clase de x con respecto a R, denotada por $R[x]$, como el conjunto*

$$R[x] = \{y \in B : xRy\}.$$

Ejemplo 5.4.

1. *Sean $A = \{a, b\}$, $B = \{x, y, z\}$ y definamos $R = \{(a, x), (a, y), (b, z)\}$, entonces tenemos que $R[a] = \{x, y\}$ y $R[b] = \{z\}$.*
2. *Para la ya conocida relación $<$ en $\mathbb{R}$ tenemos por ejemplo que $<[x] = (x, \infty)$ y para $\leq$, se tiene $\leq[x] = [x, \infty)$.*
3. *Si consideramos en $\mathbb{Z}$ la relación $x|y$, entonces la clase de x es $|[x] = \{y \in \mathbb{Z} : \exists m \in \mathbb{Z}$ tal que $y = mx\} = \{$todos los múltiplos de $x\}$.*

En estos ejemplos hemos visto que

- Una clase puede ser vacía.
- Una clase $R[x]$ no tiene que contener a x.
- Dos clases pueden intersectarse, por ejemplo en la relación $<$, dada en el ejemplo anterior, se tiene $<[1] \cap <[2] = (1, \infty) \cap (2, \infty) \neq \varnothing$.

Definición 5.5 (Dominio y Rango). *Sea R una relación de A en B. El dominio de R, denotado por* $\mathrm{dom}(R)$, *es definido como*

$$\mathrm{dom}(R) = \{x : \text{ existe } y \text{ tal que } (x, y) \in R\}.$$

El rango de R, denotado como $\mathrm{ran}(R)$, *es definido como*

$$\mathrm{ran}(R) = \{y : \text{ existe } x \text{ tal que } (x, y) \in R\}.$$

Ejemplo 5.6. *Sea R la relación definida en el conjunto de los números reales por xRy si y sólo si $x^2 + y^2 = 1$. Graficamente R es un circunferencia de centro en el origen y radio 1. En este caso es fácil ver que* $\mathrm{dom}(R) = \{x \in \mathbb{R} : -1 \leq x \leq 1\}$ *y* $\mathrm{ran}(R) = \{y \in \mathbb{R} : -1 \leq y \leq 1\}$. *Probaremos la primera igualdad, la segunda es dejada como ejercicio al lector. Para eso tome $x \in \mathrm{dom}(R)$, entonces existe un número real y tal que $(x, y) \in R$, luego $x^2 + y^2 = 1$, entonces $0 \leq x^2 = 1 - y^2$, de lo que podemos concluir que $-1 \leq y \leq 1$. Como $x^2 = 1 - y^2$, también se obtiene que $-1 \leq x \leq 1$. Lo que muestra que* $\mathrm{dom}(R) \subseteq \{x \in \mathbb{R} : -1 \leq x \leq 1\}$. *Para mostrar la otra contenencia suponga que $x \in \mathbb{R}$ y $-1 \leq x \leq 1$. Ahora defina $y := 1 - x^2$, como $-1 \leq x \leq 1$ se tiene que y es un número real y es claro que $x^2 + y^2 = 1$, lo que implica $(x, y) \in R$, luego $x \in \mathrm{dom}(R)$. Por tanto* $\{x \in \mathbb{R} : -1 \leq x \leq 1\} \subseteq \mathrm{dom}(R)$.

Definición 5.7 (Relación Identidad). *Sea A un conjunto. La relación identidad en A, denotada por I_A, es definida como*

$$I_A = \{(x, x) \in A \times A\}.$$

Ahora analizaremos ciertas relaciones especiales.

Definición 5.8. *Sea A un conjunto no vacío y sea R una relación en A. Entonces,*

1. *R es reflexiva si y sólo si xRx, para todo $x \in A$.*
2. *R es simétrica si y sólo si xRy implica que yRx, para todo $x, y \in A$.*
3. *R es transitiva si y sólo si xRy y yRz implica que xRz, para todo $x, y, z \in A$.*
4. *Si R es reflexiva, simétrica y transitiva, se dice que R es una relación de equivalencia.*
5. *R es antisimétrica si y sólo si xRy y yRx implica que $x = y$, para todo $x, y \in A$*

Ejemplo 5.9.
1. *La relación $\subseteq$ en una familia de conjuntos es reflexiva, transitiva y antisimétrica, pero no simétrica. En efecto, por parte (4) del Teorema 3.12 se tiene que $A \subseteq A$, para todo conjunto A, luego $\subseteq$ es reflexiva. Si $A \subseteq B$ y $B \subseteq C$, por parte (6) del Teorema 3.12 se obtiene que $A \subseteq C$, lo que implica que $\subseteq$ es transitiva y si $A \subseteq B$ y $B \subseteq A$, por parte (5) del Teorema 3.12 se obtiene que $A = B$, lo que implica que $\subseteq$ es antisimétrica. Para ver que $\subseteq$ no es simétrica note que $A = \{1, 2\}$ y $B = \{1, 2, 3\}$ son conjuntos tales que $A \subseteq B$, pero no es cierto que $B \subseteq A$.*
2. *La relación $\leq$ en $\mathbb{R}$ es reflexiva, transitiva y antisimétrica, pero no es simétrica. En efecto, es claro que $a \leq a$, para todo $a \in \mathbb{R}$, por tanto $\leq$ es reflexiva. Si $a \leq b$ y $b \leq a$, también sabemos que eso implica que $a = b$, por tanto $\leq$ es antisimétrica. Si $a \leq b$ y $b \leq c$, sabemos que eso implica que $a \leq c$, por tanto $\leq$ es transitiva. Para ver que no es simétrica, note que $1, 2 \in \mathbb{R}$ y $1 \leq 2$, pero no es cierto que $2 \leq 1$, así que $\leq$ no es simétrica.*
3. *La relación $<$ en $\mathbb{R}$ es sólo transitiva, demostrar este hecho queda como ejercicio al lector.*
4. *Sea $A = \{1, 2, 3\}$, $R_1 = \{(1, 2), (2, 1), (1, 3), (3, 1)\}$ es simétrica, pero no es reflexiva ni transitiva. $R_2 = \{(1, 1), (1, 2), (2, 2), (3, 3), (3, 1)\}$ es reflexiva, pero no es simétrica y tampoco transitiva. La prueba de las propiedades de R_1 y R_2 enunciadas anteriormente es muy tediosa y por tanto son dejadas como ejercicio al lector.*

Definición 5.10 (Relación Inversa)**.** *Sea R una relación de A en B. La inversa de R, denotada por R^{-1}, se define como*

$$R^{-1} = \{(x, y) : \ (y, x) \in R\}.$$

Es claro que $R^{-1} \subseteq B \times A$ y que $(x, y) \in R^{-1}$ si y sólo si $(y, x) \in R$.

Ejemplo 5.11. *Si R es la relación en los números reales definida por xRy si y sólo si $x \leq y$, entonces R^{-1} es una relación definida en los número reales como $xR^{-1}y$ si y sólo si $y \leq x$.*

La prueba del siguiente teorema es dejada como ejercicio al lector.

Teorema 5.12. *Sea R una relación en un conjunto A. Entonces*

1. *Si R es reflexiva en A, entonces R^{-1} es reflexiva en A.*
2. *Si R es simétrica en A, entonces R^{-1} es simétrica en A.*

3. *Si R es transitiva en A, entonces R^{-1} es transitiva en A.*

4. *Si R es antisimétrica en A, entonces R^{-1} es antisimétrica en A.*

Definición 5.13 (Composición). *Sean S una relación de A en B y R una relación de B en C. La composición de R con S, denotada $R \circ S$, es definidad como*

$$R \circ S = \{(x, z) : \text{ existe } y \text{ tal que } [xSy \ \wedge \ yRz]\}.$$

Ejemplo 5.14. *Sean $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ y $C = \{\alpha, \beta, \gamma\}$ y considere $S = \{(1, a), (2, b), (3, c)\}$, $R = \{(a, \alpha), (b, \beta), (c, \gamma)\}$. Entonces, S es una relación de A en B y R es una relación de B en C. La pareja ordenada $(1, \alpha)$ es un miembro de $R \circ S$ porque $(1, a) \in S$ y $(a, \alpha) \in R$. Es fácil ver que*

$$R \circ S = \{(1, \alpha), (2, \beta), (3, \gamma)\} \quad y \quad S \circ R = \varnothing.$$

Teorema 5.15. *Sean R, S y T relaciones en un conjunto A. Entonces*

1. $(R \circ S) \circ T = R \circ (S \circ T)$.

2. $(R^{-1})^{-1} = R$.

3. $I_A \circ R = R \circ I_A = R$.

4. $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

Prueba: Sólo haremos algunas de las pruebas y las restantes serán dejadas como ejercicio al lector.
1.

$$\begin{aligned}(x, y) \in (R \circ S) \circ T &\leftrightarrow (\exists\ z)[(x, z) \in T \wedge (z, y) \in (R \circ S)] \\ &\leftrightarrow (\exists\ z)(\exists\ w)[(x, z) \in T \wedge (z, w) \in S \wedge (w, y) \in R] \\ &\leftrightarrow (\exists\ w)(\exists\ z)[(x, z) \in T \wedge (z, w) \in S \wedge (w, y) \in R] \\ &\leftrightarrow (\exists\ w)[(x, w) \in (S \circ T) \wedge (w, y) \in R] \\ &\leftrightarrow (x, y) \in R \circ (S \circ T).\end{aligned}$$

2. $(x, y) \in (R^{-1})^{-1} \leftrightarrow (y, x) \in R^{-1} \leftrightarrow (x, y) \in R$. □

Ahora que ya definimos la inversa de una relación podemos relacionarla con los conceptos de dominio y rango.

Teorema 5.16. *Sean S y T relaciones, entonces*

1. $\text{dom}(S) = \text{ran}(S^{-1})$.

2. $\text{ran}(S) = \text{dom}(S^{-1})$.

3. $\text{dom}(S \circ T) \subseteq \text{dom}(T)$.

4. $\text{ran}(S \circ T) \subseteq \text{ran}(S)$.

Prueba: Sólo haremos algunas de las pruebas y las restantes serán dejadas como ejercicio al lector.

1. $x \in \text{dom}(S) \leftrightarrow (\exists\, y)[(x,y) \in S] \leftrightarrow (\exists\, y)[(y,x) \in S^{-1}] \leftrightarrow x \in \text{ran}(S^{-1})$.

3. $x \in \text{dom}(S \circ T) \leftrightarrow (\exists\, y)[(x,y) \in (S \circ T)] \leftrightarrow (\exists\, y)(\exists\, z)[(x,z) \in T \wedge (z,y) \in S]$
$\rightarrow (\exists\, z)[(x,z) \in T] \leftrightarrow x \in \text{dom}(T)$. □

La prueba del siguiente corolario es dejada como ejercicio al lector.

Corolario 5.17. *Sean S y T relaciones. Si* $\text{ran}(T) \subseteq \text{dom}(S)$, *entonces* $\text{dom}(S \circ T) = \text{dom}(T)$.

5.2. Relaciones de Equivalencia

Recordemos la definición de relación de equivalencia.

Definición 5.18. *Sean A un conjunto y $\sim$ una relación en (o sobre) A. Decimos que $\sim$ es una relación de equivalencia si $\sim$ es reflexiva, simétrica y transitiva.*

Ejemplo 5.19.

1. *Sea $n \in \mathbb{N}$. Si $a, b \in \mathbb{Z}$, decimos que a es congruente con b módulo n, denotado $a \equiv b (mod\, n)$, si existe $k \in \mathbb{Z}$ tal que $a - b = kn$. Es fácil ver que $\equiv (mod\, n)$ es una relación de equivalencia. En efecto, si $a \in \mathbb{Z}$ es claro que $a - a = 0 = 0n$, lo que implica que $a \equiv a (mod\, n)$ y por tanto $\equiv (mod\, n)$ es reflexiva. Suponga que $a \equiv b (mod\, n)$, entonces existe $k \in \mathbb{Z}$ tal que $a - b = kn$, luego $b - a = -kn$ y como $-k \in \mathbb{Z}$ se tiene que $b \equiv a (mod\, n)$, lo que implica que $\equiv (mod\, n)$ es simétrica. Finalmente, suponga que $a \equiv b (mod\, n)$ y $b \equiv c (mod\, n)$, entonces existen $k, m \in \mathbb{Z}$ tales que $a - b = kn$ y $b - c = mn$, después de sumar las dos últimas igualdades se obtiene que $a - c = (k + m)n$ y como $k + m \in \mathbb{Z}$ se llega a que $a \equiv c (mod\, n)$ y por tanto $\equiv (mod\, n)$ es transitiva.*

2. *La igualdad entre elementos de $\mathbb{R}$ es una relación de equivalencia.*

3. *La relación de semejanza en triángulos, en el conjunto de todos los triángulos, es una relación de equivalencia.*

4. *Tener la misma edad, en el conjunto de todas las personas de un país, también es una relación de equivalencia.*

Definición 5.20. *Sean A un conjunto no vacío y $\sim$ una relación de equivalencia en A. Considere $x \in A$, la clase de x con respecto a $\sim$ son llamadas clases de equivalencia y serán denotadas simplemente por $[x]$.*

Definición 5.21 (Conjunto Cociente)**.** *El conjunto cociente de A por la relación $\sim$ es el conjunto de todas las clases de equivalencia de A, con respecto a $\sim$. Lo denotaremos por $A/\sim$, más exactamente,*

$$A/\sim = \{[x] : x \in A\}.$$

Ejemplo 5.22. *Sea P el conjunto de todos los estudiantes de la universidad. Sea $\sim$ la relación en P dada por*

$$x \sim y \text{ si y sólo si } x \text{ e } y \text{ tienen el mismo apellido.}$$

Claramente $\sim$ es una relación de equivalencia. Cada clase de equivalencia corresponde a un apellido [Pérez], [Tejada], [Jiménez], [Banquet],... Luego

$$P/\sim = \{[\text{Pérez}], [\text{Tejada}], [\text{Jiménez}], [\text{Banquet}], \ldots\}.$$

Teorema 5.23. *Sea A un conjunto no vacío y sea $\sim$ una relación de equivalencia en A.*

1. *Para todo $x \in A$, se tiene que $[x] \neq \varnothing$.*
2. *Sean $x, y \in A$. Si $x \sim y$, entonces $[x] = [y]$. Si $x \nsim y$, entonces $[x] \cap [y] = \varnothing$*
3. $\bigcup_{x \in A}[x] = A$.

Prueba: Si $\sim$ es una relación de equivalencia, entonces $\sim$ es reflexiva, simétrica y transitiva.

1. Sea $x \in A$. Como $x \sim x$, entonces $x \in [x]$, lo que termina la prueba.
2. Sean $x, y \in A$. Supongamos que $x \sim y$. Veamos que $[x] = [y]$ es decir, veamos que $[x] \subseteq [y]$ y $[y] \subseteq [x]$. Sea $z \in [x]$, entonces $x \sim z$, como $x \sim y$, entonces $y \sim x$ (propiedad de simetría), luego $y \sim z$ (propiedad de transitividad), así que $z \in [y]$. De forma similar se prueba la otra contenencia, por tanto $[x] = [y]$.

 Ahora supongamos que $x \nsim y$ y veamos que $[x] \cap [y] = \varnothing$. Razonemos por contradicción y supongamos que $[x] \cap [y] \neq \varnothing$. Luego existe $z \in [x] \cap [y]$. Es decir, $z \in [x]$ y $z \in [y]$. Entonces $x \sim y$ y $y \sim z$. Por simetría $z \sim y$ luego aplicando la propiedad transitiva $x \sim y$, lo cual es absurdo, pues va en contra de la hipótesis inicial. Por tanto $[x] \cap [y] = \varnothing$.
3. Veamos que $\cup_{x \in A}[x] = A$.
 "$\subseteq$" Como para cada $x \in A$, $[x] = \{z \in A : x \sim z\}$, entonces $[x] \subseteq A$, para todo $x \in A$, consecuentemente $\cup_{x \in A}[x] \subseteq A$.
 "$\supseteq$" Sea $z \in A$, veamos que $z \in \cup_{x \in A}[x]$. En efecto $z \in [z]$ pues $z \sim z$ (reflexividad), luego si $x = z$, tenemos que existe $x \in A$ tal que $z \in [x]$, luego $z \in \cup_{x \in A}[x]$. □

Corolario 5.24. *Sean A un conjunto no vacío y $\sim$ una relación de equivalencia en A. Considere $x, y \in A$. Entonces $[x] = [y]$ si y sólo si $x \sim y$.*

Definición 5.25. *Sea A un conjunto no vacío. Una partición de A es una colección $\mathscr{P}$ de subconjuntos no vacíos de A tales que:*

1. *$P \cap Q = \varnothing$ cuando $P, Q \in D$ y $P \neq Q$.*
2. $\bigcup_{P \in \mathscr{P}} P = A$.

Corolario 5.26. *Sean A un conjunto no vacío y $\sim$ una relación de equivalencia en A. Entonces $A/\sim$ es una partición de A.*

5.3. Ejercicios

1. Para cada una de las siguientes relaciones en $\mathbb{Z}$, encuentre $R[3]$, $R[-3]$ y $R[6]$

 (i) Sea R la relación dada por aRb si y sólo si $a = |b|$, para todo $a, b \in \mathbb{Z}$.

 (ii) Sea R la relación dada por aRb si y sólo si $a|b$, para todo $a, b \in \mathbb{Z}$.

 (iii) Sea R la relación dada por aRb si y sólo si $b|a$, para todo $a, b \in \mathbb{Z}$.

 (iv) Sea R la relación dada por aRb si y sólo si $a + b = 7$, para todo $a, b \in \mathbb{Z}$.

 (vi) Sea R la relación dada por aRb si y sólo si $a - b \in \mathbb{Q}$, para todo $a, b \in \mathbb{R}$.

 (vii) Sea R la relación dada por aRb si y sólo si $ab \geq 0$, para todo $a, b \in \mathbb{R}$.

2. Defina la siguiente relación sobre $\mathscr{P}(\mathbb{N})$, XRY si $X \cap Y \neq \varnothing$. Determine si R es reflexiva, simétrica o transitiva.

3. Para cada una de las siguientes relaciones en $\mathbb{R}^2$, dé una descripción geométrica de $S[(0,0)]$ y $S[(3,4)]$.

 (i) Sea S la relación dada por $(x, y)S(z, w)$ si y sólo si $y = 3w$, para todo $(x, y), (z, w) \in \mathbb{R}^2$.

 (ii) Sea S la relación dada por $(x, y)S(z, w)$ si y sólo si $x^2 + 3y^2 = 7z^2 + w^2$, para todo $(x, y), (z, w) \in \mathbb{R}^2$.

 (iii) Sea S la relación dada por $(x, y)S(z, w)$ si y sólo si $x = z$ o $y = w$, para todo $(x, y), (z, w) \in \mathbb{R}^2$.

4. Considere la relación definida en $\mathbb{Z} \times \mathbb{Z}$, como $(x, y)R(z, w)$ si $x + y = z + w$.

 a) Determine si R es reflexiva, simétrica o transitiva.

 b) Hallar R[(1,1)].

 c) Calcular el espacio cociente de $\mathbb{Z} \times \mathbb{Z}/R$.

5. Considere la relación definida en $\mathbb{R} \times \mathbb{R}$, como $(x, y)R(z, w)$ si $xy = zw$.

 a) Determine si R es reflexiva, simétrica o transitiva.

 b) Hallar R[(1,1)].

 c) Hallar R[(0,0)].

 d) Calcular el espacio cociente de $\mathbb{R} \times \mathbb{R}/R$.

6. Pruebe el Teorema 5.12.

7. Termine de probar el Teorema 5.15.

8. Termine de probar el Teorema 5.16

9. Pruebe el Corolario 5.17.

10. Sea $A = \{1, 2, 3\}$. ¿Es cada uno de las siguientes relaciones en A reflexiva, simétrica o transitiva?

(i) $M = \{(3,3),(2,2),(1,2),(2,1)\}$

(ii) $N = \{(1,1),(2,2),(3,3),(1,2)\}$

(iii) $O = \{(1,1),(2,2),(1,2)\}$

(iv) $P = \{(3,3),(2,2),(1,1)\}$

(v) $Q = \{(1,2),(2,1),(1,3),(3,1),(1,1)\}$

(vi) $R = \{(1,2),(2,3),(3,1)\}$

(vii) $T = \{(1,1),(1,2),(2,2),(2,3),(3,3),(1,3)\}$

11. ¿Es cada una de las siguientes relaciones reflexiva, simétrica y/o transitiva?

(i) Sea S la relación en $\mathbb{R}$ dada por xSy si y sólo si $y = |x|$, para todo $x, y \in \mathbb{R}$.

(ii) Sea D la relación dada por aDb si y sólo si $a|b$, para todo $a, b \in \mathbb{Z}$.

(iii) Sea T la relación en $\mathbb{Z} \times \mathbb{Z}$ definida por $(x,y)T(z,w)$ si y sólo si (x,y) y (z,w) están ambos en una linea en $\mathbb{R}^2$ con pendiente un entero, para todo $(x,y),(z,w) \in \mathbb{R}^2$.

12. Muestre que la relación $\equiv \pmod{n}$ es una relación de equivalencia en $\mathbb{Z}$. Encuentre [23], [15] y [14] cuando $n = 12$

13. Encuentre el dominio y el rango de cada una de las siguientes relaciones.

a) Para todo $x, y \in \mathbb{R}$, xRy si y sólo si $|x| = |y|$.

b) Para todo $x, y \in \mathbb{R}$, xRy si y sólo si $x = |y|$.

c) Para todo $x, y \in \mathbb{R}$, xRy si y sólo si $x + y = 1$.

d) Para todo $x, y \in \mathbb{R}$, xRy si y sólo si $\lfloor x \rfloor = \lfloor y \rfloor$.

e) Para todo $x, y \in \mathbb{N}$, xRy si y sólo si $x|y$.

14. Construya una relación R en el conjunto $A = \{1,2,3\}$ tal que satisfaga las condiciones dadas

a) R es reflexiva en A pero no simétrica.

b) R es simétrica pero no reflexiva en A.

c) R es simétrica pero no transitiva.

d) R es transitiva pero no simétrica.

15. Sean R, S y T relaciones en un conjunto A. Pruebe cada una de las siguientes afirmaciones.

a) R es simétrica si y sólo si $R = R^{-1}$.

b) $R \cup R^{-1}$ es simétrica.

c) R es reflexiva en A si y sólo si $I_A \subseteq R$.

d) R es antisimétrica si y sólo si $R \cap R^{-1} \subseteq I_A$.

e) R es transitiva si y sólo si $R \circ R \subseteq R$.

16. Sean R y S relaciones en un conjunto A. Pruebe o dé un contraejemplo para cada una de las siguientes afirmaciones.

a) Si R y S son reflexivas en A, entonces $R \cup S$ es reflexiva en A.

b) Si R y S son simétricas, entonces $R \cup S$ es simétrica.

c) Si R y S son transitivas en A, entonces $R \cup S$ es transitiva.

d) Si R y S son antisimétricas, entonces $R \cup S$ es antisimétrica.

e) Si R y S son reflexivas en A, entonces $R \cap S$ es reflexiva en A.

f) Si R y S son simétricas, entonces $R \cap S$ es simétrica.

g) Si R y S son transitivas en A, entonces $R \cap S$ es transitiva.

h) Si R y S son antisimétricas, entonces $R \cap S$ es antisimétrica.

i) $\text{dom}(R \cup S) = \text{dom}(R) \cup \text{dom}(S)$.

j) $\text{ran}(R \cup S) = \text{ran}(R) \cup \text{ran}(S)$.

k) $\text{dom}(R \cap S) = \text{dom}(R) \cap \text{dom}(S)$.

l) $\text{dom}(R) - \text{dom}(S) \subseteq \text{dom}(R - S)$.

m) $\text{ran}(R) - \text{ran}(S) \subseteq \text{ran}(R - S)$.

17. Sean G, H y J relaciones en un conjunto A. Pruebe que.

a) $(H \cup J) \circ G = (H \circ G) \cup (J \circ G)$.

b) $G \circ (H \cap J) \subseteq (G \circ H) \cap (G \circ J)$.

c) $(G - H)^{-1} = G^{-1} - H^{-1}$.

d) $(G \circ H) - (G \circ J) \subseteq G \circ (H - J)$.

e) $(G \cup H)^{-1} = G^{-1} \cup H^{-1}$.

f) $(G \cap H)^{-1} = G^{-1} \cap H^{-1}$.

18. Sea $\mathscr{P}$ una partición del conjunto A. Defina la relación Q en A por xQy si y sólo si existe un conjunto $B \in \mathscr{P}$ tal que $x, y \in B$. Pruebe cada una de las siguientes afirmaciones.

a) La relación Q es reflexiva en A.

b) La relación Q es simétrica.

c) La relación Q es transitiva.

d) $A/Q = \mathscr{P}$.

Capítulo 6

El Sistema de Números Reales

Hasta aquí hemos utilizado los números reales de manera intuitiva, básicamente se han usado las propiedades aprendidas en nuestros cursos de secundaria tales como conmutatividad, asociatividad, existencia de neutros y otras, pero en realidad no hemos definidos los números reales de manera rigurosa. Hay varias formas de construir "el" sistema de los números reales, por ejemplo, comenzando con los números naturales podemos definir los enteros y luego los números racionales de forma algebraica, y finalmente podemos construir los números reales como clases de equivalencia de sus sucesiones de Cauchy de números racionales. También es posible usar cortes de Dedekind, los cuales son ciertos subconjuntos de números racionales. Otra posibilidad es comenzar con una rigurosa axiomatización de la Geometría Euclidiana y entonces definir el sistema de números reales geometricamente. Por cuestiones de simplicidad y rapidez en este libro hemos decidido introducir los números reales de manera axiomática, esto es, aceptaremos como verdaderas varias reglas básicas (los cuales llamaremos axiomas) y a partir de estos axiomas deduciremos todas las propiedades algebraicas que conocemos sobre los números reales. Como es bien conocido existe un teorema de la matemática avanzada que dice que existe un solo *campo ordenado completo*, aceptando la veracidad de este teorema (cuya prueba se escapa a los objetivos de este libro) hemos decidido definir primero los números reales y después hacer toda nuestra teoría sobre campos ordenados completos, lo cual creemos no causará muchos inconvenientes al lector.

6.1. Axiomas de un Campo Ordenado

Notaremos el conjunto de los números reales por $\mathbb{R}$ y aceptaremos que en él existe una relación de equivalencia designada por $=$. Además, asumiremos como axiomas, esto es, sin dar una prueba, las siguientes propiedades simples de los números reales.

A Axiomas de Campo: Existen funciones $+$ y $\cdot$ definidas en $\mathbb{R} \times \mathbb{R}$, las cuales satisfacen las siguientes propiedades:

I. (Clausurativa) La suma $x + y$ y el producto $x \cdot y$ de cualquier dos números reales x e y, son ellos mismos números reales. En símbolos

$$(\forall x, y \in \mathbb{R})(x + y \in \mathbb{R} \quad \wedge \quad x \cdot y \in \mathbb{R})$$

II. (Conmutativa) $(\forall x, y \in \mathbb{R})(x + y = y + x \quad \wedge \quad x \cdot y = y \cdot x)$

III. (Asociativa) $(\forall x, y, z \in \mathbb{R})[(x + y) + z = x + (y + z) \quad \wedge \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)]$

IV. (Existencia de elementos neutros)

(*a*) Existe un número real que denotaremos 0 y llamaremos "cero" , tal que para todo $x \in \mathbb{R}$, $x + 0 = x$.

(*b*) Existe un número real que denotaremos 1 y llamaremos "uno", tal que $1 \neq 0$ y, para todo $x \in \mathbb{R}$, $x \cdot 1 = x$. En símbolos

$$(\exists 0 \in \mathbb{R})(\forall x \in \mathbb{R})(x + 0 = x)$$

$$(\exists 1 \in \mathbb{R}, 1 \neq 0)(\forall x \in \mathbb{R})(x \cdot 1 = x)$$

Los números 0 y 1 son llamados neutros para la adición y multiplicación, respectivamente.

V. (Existencia de inversos)

(*a*) Para todo número real x, existe un número real, denotado $-x$, tal que

$$x + (-x) = 0.$$

(*b*) Para todo número real x, distinto de 0, existe un número real denotado x^{-1}, tal que $x \cdot x^{-1} = 1$. En símbolos:

$$(\forall x \in \mathbb{R})(\exists - x \in \mathbb{R})[x + (-x) = 0]$$

$$(\forall x \in \mathbb{R}, x \neq 0)(\exists x^{-1} \in \mathbb{R})(x \cdot x^{-1} = 1)$$

Los números $-x$ y x^{-1} son llamados, respectivamente, el inverso aditivo (o el simétrico) y el inverso multiplicativo (o recíproco) de x.

VI. (Distributiva) $(\forall x, y, z \in \mathbb{R})\ [x \cdot (y + z) = x \cdot y + x \cdot z]$.

NOTACIÓN: Frecuentemente denotaremos $x \cdot y$ por xy

El siguiente teorema muestra que las identidades aditivas y multiplicativas son únicas.

Teorema 6.1. *Sean* $x, a \in \mathbb{R}$.

(*i*) *Si* $x + a = x$, *entonces* $a = 0$.

(*ii*) *Si* $xa = x$ *y* $x \neq 0$, *entonces* $a = 1$.

Prueba:

(*i*) Como $x \in \mathbb{R}$ existe $-x \in \mathbb{R}$ tal que $x + (-x) = 0$. De esta manera obtenemos

$$a = a + 0 = a + [x + (-x)] = (a + x) + (-x) = (x + a) + (-x) = x + (-x) = 0.$$

(*ii*) Como $x \in \mathbb{R} \setminus \{0\}$, existe $x^{-1} \in \mathbb{R}$ tal que $xx^{-1} = 1$. Luego $a = a1 = a(xx^{-1}) = (ax)x^{-1} = (xa)x^{-1} = xx^{-1} = 1$. □

El siguiente corolario nos muestra que nunca tenemos que $0 \cdot x = 1$, esta es la razón por la que 0 no tiene inverso multiplicativo, y es consecuencia de que $0 \neq 1$.

Corolario 6.2. *Sea x un número real, entonces $0x = 0$.*

Prueba: Como $x + 0x = 1x + 0x = (1 + 0)x = 1x = x$, entonces por la parte (i) del teorema anterior tenemos que $0x = 0$. □

El siguiente teorema muestra que los inversos aditivos y multiplicativos son únicos.

Teorema 6.3. *Sean $x, y \in \mathbb{R}$.*

(*i*) *Si $x + y = 0$, entonces $y = -x$.*

(*ii*) *Si $xy = 1$, entonces $y = x^{-1}$*

Prueba:

(*i*) $y = 0 + y = [x + (-x)] + y = [(-x) + x] + y = (-x) + (x + y) = -x + 0 = -x$.

(*ii*) Como $1 \neq 0$, usando el Corolario 6.2 tenemos que $x \neq 0$. Entonces existe $x^{-1} \in \mathbb{R}$ tal que $xx^{-1} = 1$. Luego $y = 1y = (xx^{-1})y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}1 = x^{-1}$. □

Los axiomas de campo son suficientes para derivar todas las propiedades algebraicas de $\mathbb{R}$, pero no lo describe completamente. El sistema de números reales también tiene una relación de orden, es decir un concepto de "menor que".

B Axiomas de Orden: Existe una relación $<$ definida en $\mathbb{R} \times \mathbb{R}$, la cual se lee menor que, y tiene las siguientes propiedades:

VII. (Tricotomia) Para cualquier par de números reales x e y se tiene que una y sólo una de las siguientes afirmaciones es cierta $x < y$ ó $y < x$ ó $x = y$.

VIII. (Transitividad) Si x, y, z son números reales, con $x < y$ y $y < z$, entonces $x < z$. En símbolos

$$(\forall x, y, z \in \mathbb{R})(x < y \quad \wedge \quad y < z \quad \text{implica} \quad x < z).$$

IX. (Monotocidad de la adición y multiplicación)

(a) $(\forall x, y, z \in \mathbb{R})(x < y \text{ implica } x + z < y + z)$.

(b) $(\forall x, y, z \in \mathbb{R})(x < y \ \wedge \ 0 < z \text{ implica } xz < yz)$.

Nota 6.4. *También se puede introducir en los reales una relación de orden de la siguiente forma. Tome como axioma la existencia de un subconjunto propio no vació de* $\mathbb{R}$*, denotado* P*, el cual satisface lo siguiente:*

(*i*) $0 \notin P$.

(*ii*) *Si* $x \in \mathbb{R}$*, entonces una y sólo una de las siguientes afirmaciones es cierta* $x \in P$*,* $-x \in P$ *ó* $x = 0$.

(*iii*) P *es cerrado bajo las operaciones* $+$ *y* $\cdot$ *de* $\mathbb{R}$*, es decir si* $x, y \in P$*, entonces* $x + y \in P$ *y* $x \cdot y \in P$.

Con este connjunto P*, una relación de orden en* $\mathbb{R}$ *se define de la siguiente forma*

$$x < y \text{ si y sólo si } \ y - x \in P.$$

Usando esta definición, todas las propiedades de las desigualdades que conocemos para los números reales pueden ser obtenidas. En este libro hemos decidido hacer un abordaje diferente sólo por cuestiones de simplicidad, se deja como ejercicio al lector mostrar que estos dos abordajes son equivalentes.

A continuación introducimos el concepto de campo, lo que nos permitirá trabajar en un contexto más general.

Definición 6.5. *Un campo* F *es cualquier conjunto de objetos con dos operaciones* $(+)$ *y* $(\cdot)$*, llamadas usualmente adición y multiplicación, definidas en* $F \times F$*, provisto de que estas operaciones y objetos cumplen las seis propiedades dadas anteriormente (I-VI).*

Si este conjunto está también equipado con una relación de orden $(<)$ *que satisface los axiomas adicionales (VII-IX), este es llamado un campo ordenado.*

En particular $\mathbb{R}$ es un campo ordenado. Cuando hablamos de un campo en general, el termino "número real" debe ser reemplazado por "elemento de F". Igualmente "0" y "1" deben ser interpretados como elementos de F.

A continuación damos un ejemplo de campo diferente a $\mathbb{R}$.

Ejemplo 6.6. *Considere* $F = \{0, 1\}$ *y las siguientes operaciones definidas en* F

$+$	0	1
0	0	1
1	1	0

$.$	0	1
0	0	0
1	0	1

Es fácil ver que F *es un campo con neutro para la suma* 0 *y para la multiplicación es* 1.

NOTACIÓN: $x > y$ significa $y < x$ y $x \leq y$ significa $x < y$ ó $x = y$; similarmente para $x \geq y$. Si $x < y$ y $y < z$, escribiremos $x < y < z$.

Definición 6.7. *Un elemento x de un campo ordenado F se dice no-negativo si $x \geq 0$, positivo si $x > 0$, no-positivo si $x \leq 0$ y negativo si $x < 0$. El elemento 0 no es positivo ni negativo.*

Los números 0 y 1 fueron introducidos en el Axioma IV, pero "oficialmente" no sabemos que significan los símbolos 2, 3, 4, ..., etc., ya que estos no han sido definidos. Como la suma ya fue definida podemos usarla para definir los naturales paso por paso, como sigue :

$$2 := 1 + 1, \quad 3 := 2 + 1, \quad 4 := 3 + 1, \quad 5 := 4 + 1, \quad \text{etc.}$$

Si este proceso se continua indefinidamente, obtenemos lo que llameremos el conjunto de los "Números Naturales". Un proceso similar puede hacerse en un campo, entonces podemos hablar de "Números Naturales" en un campo cualquiera. La definición exacta de los "Número Naturales" será dada posteriormente.

Definición 6.8. *Dados varios elementos a, b, c, d de un campo, se define*
$a + b + c = (a + b) + c$, $a + b + c + d = (a + b + c) + d$, *etc.*
Similarmente se define para la multiplicación.

6.2. Operaciones Aritméticas en un Campo

Definición 6.9. *Dados dos elementos x e y de un campo, se define la diferencia entre x e y como:*

$$x - y := x + (-y),$$

si $y \neq 0$ se define el cociente de x por y, como:

$$\frac{x}{y} := x \cdot y^{-1},$$

también denotado x/y.

Nota 6.10. *La división por 0 no esta definida, por tanto es inadmisible.*

Corolario 6.11. *La diferencia $x - y$ y el cociente x/y $(y \neq 0)$ de dos números reales x e y son números reales (similarmente la diferencia y cociente de elementos de un campo en general). En símbolos:*

$$(\forall x, y \in \mathbb{R})(x - y \in \mathbb{R}) \quad y \quad (\forall x, y \in \mathbb{R}, y \neq 0)(x/y \in \mathbb{R})$$

Corolario 6.12. *Si a, b, c pertenecen a un campo F, con $a = b$, entonces*

$$a + c = b + c \quad y \quad ac = bc.$$

En símbolos

$$(\forall a, b, c \in F)(a = b, \quad \textit{implica} \quad a + c = b + c \quad y \quad ac = bc).$$

Prueba: Por propiedades de la igualdad tenemos que $a+c = a+c$. Como $a = b$ podemos reemplazar a por b en la igualdad anterior y obtenemos que $a + c = b + c$. Similarmente $ac = bc$. □

Corolario 6.13 (Ley de Cancelación). *Si $a, b, c \in F$, entonces*

$$a + c = b + c \quad \textit{implica} \quad a = b.$$

Si además, $c \neq 0$, entonces

$$ac = bc \quad \textit{implica} \quad a = b.$$

Prueba: Suponga que $a + c = b + c$, por Corolario 6.12, podemos sumar $(-c)$ en ambos miembros de la ecuación para obtener $(a + c) + (-c) = (b + c) + (-c)$, usando la asociatividad y el hecho que $c + (-c) = 0$, obtenemos $a + 0 = b + 0$, luego $a = b$. El otro caso sigue por un argumento similar. □

Teorema 6.14. *Dados dos elementos a y b de un campo F, siempre existe un único elemento $x \in F$ tal que $a + x = b$; este elemento es igual a la diferencia $b - a$.*
Si además, $a \neq 0$, existe también un único elemento $y \in F$ tal que $ay = b$; este elemento es igual al cociente b/a. En símbolos:

$$(\forall a, b \in F)(\exists! x \in F)(a + x = b)$$

$$(\forall a, b \in F, a \neq 0)(\exists! y \in F)(ay = b)$$

Prueba: Considere $a, b \in F$ y defina $x := b - a$. Claramente $x \in F$ y satisface la ecuación $a + x = b$. En efecto,

$$a + x = a + (b - a) = (b - a) + a = [b + (-a)] + a = b + [(-a) + a] = b + 0 = b.$$

Entonces la ecuación $a + x = b$, tiene por lo menos una solución dada por $x = b - a$. Veamos ahora que esa solución es única. Supongamos que existe otra solución $x' \in F$ de la ecuación $a + x = b$. Entonces $a + x = b$ y $a + x' = b$, luego $a + x = a + x'$, por Corolario 6.13 tenemos que $x = x'$. Por tanto las dos soluciones necesariamente coinciden. La prueba de la segunda parte es similar y es dejada como ejercicio al lector. □

Corolario 6.15. *Para cualquier elemento $x \in F$, tenemos $0 - x = -x$. Si además, $x \neq 0$, entonces $\dfrac{1}{x} = x^{-1}$.*

Prueba: Por la definición de resta y el Axioma IV, tenemos que $0 - x = 0 + (-x) = -x$ similarmente, $\dfrac{1}{x} = 1 \cdot x^{-1} = x^{-1}$. □

Teorema 6.16 (Regla de los Signos). *Sean a, b elementos de un campo F, entonces*

(*i*) $-a = (-1) \cdot a$

(*ii*) $-(-a) = a$. *En particular* $(-1)(-1) = 1$.

(*iii*) $a(-b) = (-a)b = -(ab)$

(*iv*) $(-a)(-b) = ab$

(*v*) $-(a-b) = b-a.$

Prueba:

(*i*) Como $a + (-1)\cdot a = 1\cdot a + (-1)\cdot a = [1+(-1)]\cdot a = 0\cdot a = 0$, entonces por el Teorema 6.3 (*i*) tenemos que $(-1)\cdot a = -a$.

(*ii*) Como $-a + a = 0$, usando el Teorema 6.3 (*i*) tenemos que $-(-a) = a$. Ahora, por la parte (*i*), ya probada, tenemos que $(-1)\cdot(-1) = -(-1) = 1$

(*v*) En este caso

$$\begin{aligned} -(a-b) =& (-1)(a-b) = (-1)[a+(-b)] = (-1)a + (-1)(-b) = -a + [-(-b)] \\ =& -a + b = b + (-a) = b - a. \end{aligned}$$

El resto del teorema sigue de forma similar a lo hecho arriba y es dejado al lector completar los detalles. □

Teorema 6.17. *Sean a, b elementos de un campo F. Si $ab = 0$, entonces $a = 0$ o $b = 0$.*

Prueba: Supongamos que $ab = 0$ y $a \neq 0$. Entonces existe $a^{-1} \in F$ tal que $a^{-1}a = 1$. Luego

$$b = 1\cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

Lo que termina la prueba del teorema. □

6.3. Desigualdades en un Campo Ordenado y Valor Absoluto

De aquí en adelante F es considerado un campo ordenado.

Corolario 6.18. *Si x es un elemento positivo de un campo ordenado F, entonces $-x$ es negativo; y si x es negativo, entonces $-x$ es positivo.*

Prueba: Suponga que $x > 0$, por axioma IX tenemos $x + (-x) > 0 + (-x)$, luego $0 > -x$. Por tanto $-x$ es negativo. El resto de la prueba es dejada como ejercicio para el lector. □

Corolario 6.19 (Adición y Multiplicación de Desigualdades)**.** *Sean a, b, x, e y elementos de un campo F, tales que $a < b$ y $x < y$, entonces*

$$a + x < b + y.$$

Si además a, b, x e y son positivos, entonces $a < b$ y $x < y$ implican

$$ax < by.$$

Prueba: Probaremos la segunda parte del corolario, la primera parte es dejada al lector. Como $a < b$ y $x > 0$, tenemos

$$ax < bx. \tag{6.1}$$

De igual forma, como $x < y$ y $b > 0$ obtenemos que

$$bx < by. \tag{6.2}$$

Usando (6.1), (6.2) y aplicando transitividad obtenemos $ax < by$. □

Nota 6.20. *Es suficiente en el corolario anterior que x, b sean positivos, si quitamos esta hipótesis la desigualdad puede fallar por ejemplo $-2 < 3$ y $-2 < 1$, luego obtendriamos que $4 < 3$, lo cual es falso.*

Corolario 6.21. *Sean $x, y, a \in F$, donde F un campo ordenado. Suponga que $x < y$ y $a < 0$. Entonces $ax > ay$.*

Teorema 6.22. *Sean F un campo ordenado y $a, b \in F$.*

(*i*) *Si $a \neq 0$, entonces $a \cdot a > 0$ y $(-a)^{-1} = -a^{-1}$. En particular $1 > 0$.*

(*ii*) *Si $a > 0$, entonces $a^{-1} > 0$.*

(*iii*) *Si $a > 0$ y $b > 0$, entonces $a \cdot b > 0$.*

(*iv*) *Si $a < b$ y $a > 0$, entonces $b^{-1} < a^{-1}$.*

(*v*) *Si $a < b$ y $b < 0$, entonces $b^{-1} < a^{-1}$.*

Prueba:

(*i*) Suponga que $a \neq 0$, por tricotomía tenemos que $a > 0$ ó $a < 0$. Si $a > 0$, entonces multiplicando por a, obtenemos $a \cdot a > 0 \cdot a$, luego $a^2 > 0$. Si $a < 0$, entonces por Corolario 6.18, $-a > 0$, entonces $(-a) \cdot (-a) > 0 \cdot (-a)$, por el Teorema 6.16 tenemos que $a \cdot a > 0$, por tanto $a^2 > 0$. Ahora, como $1 \neq 0$ y $1 \cdot 1 > 0$, entonces $1 > 0$. El resto de la prueba de (i) es dejada como ejercicio al lector.

(*ii*) Como $a > 0$, entonces $a^{-1} \neq 0$. Luego por (i) se tiene que $a^{-1} \cdot a^{-1} > 0$, por tanto $a \cdot (a^{-1} \cdot a^{-1}) > 0 \cdot a = 0$. Asi, usando la asociatividad y el hecho que $a \cdot a^{-1} = 1$, tenemos que $a^{-1} > 0$.

(*iv*) Como a y b son positivos y la parte (ii) tenemos que $a^{-1}, b^{-1} > 0$. Usando la parte (iii) se tiene que $b^{-1} \cdot a^{-1} > 0$. Ahora, como $a < b$, tenemos que

$$(b^{-1} \cdot a^{-1}) \cdot a < (b^{-1} \cdot a^{-1}) \cdot b.$$

Por la asociatividad y conmutatividad llegamos a que $b^{-1} \cdot (a^{-1} \cdot a) < (b \cdot b^{-1}) \cdot a^{-1}$. De esta última desigualdad se deduce inmediatamente el resultado deseado. El resto de los items quedan como ejercicio al lector. □

Definición 6.23 (Valor Absoluto). *Dado un elemento x de un campo F, definimos su valor absoluto, denotado $|x|$, como sigue si $x \geq 0$, entonces $|x| = x$; si $x < 0$, entonces $|x| = -x$. En forma mas compacta sería*

$$|x| = \begin{cases} -x & si\ x < 0, \\ x & si\ x \geq 0. \end{cases}$$

Teorema 6.24. *Sean a y b elementos de un campo ordenado F. Entonces*

(*i*) *Positividad:* $|a| \geq 0$ *y* $|a| = 0$ *si y sólo si* $a = 0$.

(*ii*) *Multiplicatividad:* $|a \cdot b| = |a| \cdot |b|$. *Si además* $b \neq 0$, *entonces* $\frac{|a|}{|b|} = |\frac{a}{b}|$.

(*iii*) *Simetria:* $|a - b| = |b - a|$.

(*iv*) $-|a| \leq a \leq |a|$.

Prueba:

(*i*) Tenemos dos casos, si $a \geq 0$, $|a| = a \geq 0$ y si $a < 0$, entonces por Corolario 6.18, $-a > 0$ y como $|a| = -a$, tenemos que $|a| > 0$. En cualquier caso tenemos que $|a| \geq 0$. Ahora, si $a = 0$, es claro que $|a| = 0$. Suponga que $|a| = 0$, entonces por definición $\pm a = 0$. Como $\pm a = (\pm 1) \cdot a$ y $\pm 1 \neq 0$, tenemos que $a = 0$.

(*ii*) Ejercicio para el lector.

(*iii*) $|a - b| = |(-1)(b - a)| = |-1| \cdot |b - a| = 1 \cdot |b - a| = |b - a|$.

(*iv*) Si $a \geq 0$, entonces $|a| = a$; $-|a| = -a \leq 0 \leq a$, entonces $-|a| \leq a \leq |a|$. Si $a < 0$, entonces $|a| > a$ y $|a| = -a$, entonces $-|a| \leq a \leq |a|$. □

Corolario 6.25. *Para cualesquiera elementos x e y de un campo ordenado F, tenemos que*

$$|x| < y \quad si\ y\ sólo\ si \quad -y < x < y.$$

Prueba: "⇒" Supongamos que $|x| < y$, por Teorema 6.24 (iv), tenemos

$$x \leq |x| < y,$$

entonces $x < y$. Falta probar que $x > -y$. Como $|x| < y$, se tiene $-y < -|x|$ y de nuevo por Teorema 6.24 (iv) se obtiene $-y < -|x| \leq x$, así que $-y < x$. Por tanto $-y < x < y$.
"⇐" Se deja como ejercicio al lector. □

Corolario 6.26. *Sea F un campo ordenado. Si $a, b \in F$, entonces*

(*i*) *Desigualdad Triangular:* $|a + b| \leq |a| + |b|$

(*ii*) $||a| - |b|| \leq |a - b|$.

(*iii*) $|a| - |b| \leq |a \pm b| \leq |a| + |b|$.

Prueba: El item (*iii*) es dejado como ejercicio al lector.

(*i*) Sabemos que $-|a| \leq a \leq |a|$ y $-|b| \leq b \leq |b|$, luego sumando estas dos desigualdades obtenemos

$$-(|a| + |b|) \leq a + b \leq |a| + |b|.$$

Por tanto, usando el Corolario 6.25 se tiene que $|a + b| \leq |a| + |b|$.

(*ii*) Usando la desigualdad triangular tenemos que $|a| = |(a - b) + b| \leq |a - b| + |b|$, entonces

$$|a| - |b| \leq |a - b|. \tag{6.3}$$

Si intercambiamos a por b en el argumento anterior tendremos que

$$|b| - |a| \leq |b - a| = |-(a - b)| = |a - b|,$$

entonces

$$-|a - b| \leq |a| - |b| \tag{6.4}$$

De (6.3), (6.4) y el Corolario 6.25, obtenemos el resultado deseado. □

Corolario 6.27. *Considere dos elementos a y b de un campo ordenado F, tales que $a < b$, entonces existe un elemento $x \in F$ tal que $a < x < b$.*

Prueba: Defina $x := \frac{1}{2}(a + b)$. Claramente $x \in F$. Es fácil probar que $a < x < b$. Los detalles son dejados al lector. □

Teorema 6.28. *Sean $x, y, a \in F$, donde F es un campo ordenado.*

(*i*) *$x < y + \epsilon$ para todo $\epsilon > 0$ si y sólo si $x \leq y$.*

(*ii*) *$x > y - \epsilon$ para todo $\epsilon > 0$ si y sólo si $x \geq y$.*

(*iii*) *$|a| < \epsilon$ para todo $\epsilon > 0$ si y sólo si $a = 0$.*

Prueba:

(*i*) *Suponga que $x > y$. Considere $\epsilon_0 := x - y > 0$. por hipótesis tenemos que*

$$x < y + \epsilon_0 = y + (x - y) = x,$$

luego $x < x$, lo cual es absurdo. Por tanto $x \leq y$. Ahora, si $x \leq y$ y $\epsilon > 0$, tenemos que $x < x + \epsilon \leq y + \epsilon$.

(*ii*) *$x > y - \epsilon$ si y sólo si $x + \epsilon > y$ si y solo si $y < x + \epsilon$ si y sólo si $y \leq x$.*

(*iii*) *$|a| < \epsilon$ para todo $\epsilon > 0$ si y sólo si $|a| < 0 + \epsilon$ para todo $\epsilon > 0$, si y sólo si $|a| \leq 0$, si y sólo si $a = 0$.* □

6.4. Números Naturales e Inducción

Al final de la Sección 6.1 se mostró como construir los números naturales $1, 2, 3,...$ comenzando con 1 y entonces adicionando 1 a cada número precedente para obtener el siguiente. Este proceso también aplica a cualquier campo F y de esa forma se obtienen los llamados números naturales de F. El conjunto de tales elementos es denotado $\mathbb{N}$. Nótese que por la construcción $n+1 \in \mathbb{N}$ siempre que $n \in \mathbb{N}$. Podemos mirar todo esto de otra forma.

Definición 6.29 (Conjunto Inductivo)**.** *Un subconjunto S de un campo F es llamado inductivo si*

(1) $1 \in S$ *y*

(2) *para todo $x \in S$, tenemos que $x+1 \in S$.*

Un ejemplo de un conjunto inductivo es F. También $\mathbb{R}^+$ es un subconjunto inductivo de $\mathbb{R}$.

Definición 6.30 (Números Naturales)**.** *Definimos el conjunto de los números Naturales en un campo F, denotado $\mathbb{N}$, como la intersección de todos los subconjuntos inductivos de F, i.e.,*

$$\mathbb{N} = \bigcap \{S : S \text{ subconjunto inductivo de } F\}.$$

Por tanto $x \in \mathbb{N} \Leftrightarrow x \in S$, para todo subconjunto inductivo S de F.
Llamaremos números Enteros en un campo F, al conjunto

$$\mathbb{Z} := \{k \in F : k = 0, -k \in \mathbb{N} \quad \acute{o} \quad k \in \mathbb{N}\}.$$

Teorema 6.31. *$\mathbb{N}$ es no vacío e inductivo. De hecho es el "menor" subconjunto inductivo de F (i.e., está contenido en cualquier subconjunto inductivo de F).*

Prueba: Como $1 \in S$ para todo conjunto inductivo $S \subset F$, entonces $1 \in \mathbb{N}$, lo que muestra que $\mathbb{N}$ es no vacío. Sea $x \in \mathbb{N}$, por la definición de $\mathbb{N}$, tenemos que x está en todo conjunto inductivo S, como S es inductivo se tiene que $x+1 \in S$, por tanto $x+1 \in \mathbb{N}$. Ahora, sean $S \subset F$ un subconjunto inductivo de F y $x \in \mathbb{N}$. Luego por la definición de $\mathbb{N}$, $x \in S$. Por tanto $\mathbb{N} \subset S$. □

El teorema anterior es usado frecuentemente para probar proposiciones generales en los números naturales, el procedimiento es el siguiente: Para probar que una fórmula o proposición $p(n)$ vale para todo natural n, primero definimos un conjunto

$$E := \{n \in \mathbb{N} : p(n) \text{ es cierta}\},$$

luego verificamos que $1 \in E$ es decir, mostramos que $p(n)$ es cierta para $n = 1$. Inmediatamente mostramos que $m \in E$ implica $m+1 \in E$, esto es, si $p(n)$ vale para algún valor $n = m$, entonces $p(n)$ vale también para $n = m+1$. Una vez esto se ha establecido lo que se ha probado es que E es un subconjunto inductivo de F, así el Teorema 6.31 asegura que $\mathbb{N} \subseteq E$ y como $E \subseteq \mathbb{N}$, tenemos que $E = \mathbb{N}$. Por tanto $p(n)$ vale para todo $n \in \mathbb{N}$. Este método de demostración es llamado Principio de Inducción Matemática (P. I. M.), el cual se formula de la siguiente forma: Si $E \subseteq \mathbb{N}$ tal que $1 \in E$ y $x \in E$ implica $x+1 \in E$, entonces $E = \mathbb{N}$. Este método de demostración será usado de aquí en adelante pata obtener algunas propiedades de lo números naturales.

Teorema 6.32. (*i*) *Dado* $n \in \mathbb{Z}$ *una y sólo una de las siguientes afirmaciones se cumple* $n > 0, n < 0$ *ó* $n = 0$.

(*ii*) $n \in \mathbb{N}$ *implica* $n \geq 1$

(*iii*) *Si* $n \in \mathbb{N}$, *entonces* $n - 1 = 0$ *ó* $n - 1 \in \mathbb{N}$

(*iv*) *Si* $n \in \mathbb{Z}$ *y* $n > 0$, *entonces* $n \in \mathbb{N}$

(*v*) *Si* $p \in \mathbb{Z}$, *entonces* $p - 1 \in \mathbb{Z}$

(*vi*) *Si* $m, n \in \mathbb{N}$ *y* $m < n$, *entonces* $m + 1 \leq n$

Prueba:

(*i*) Como F^+ es inductivo, entonces $\mathbb{N} \subseteq F^+$, es decir los números naturales son positivos. Por la definición de $\mathbb{Z}$, dado $n \in \mathbb{Z}$ una de las siguientes afirmaciones se cumple: $n \in \mathbb{N}$, $-n \in \mathbb{N}$ ó $n = 0$; es decir $n > 0, n < 0$ ó $n = 0$. Ahora bien, la propiedad de Tricotomia implica que sólo una de estas condiciones se puede cumplir para $n \in \mathbb{Z}$ dado.

(*ii*) Es claro que el conjunto $E := \{x \in F : x \geq 1\}$ es inductivo, por tanto $\mathbb{N} \subseteq E$.

(*iii*) Defina $E := \{n \in \mathbb{N} : n - 1 = 0 \text{ ó } n - 1 \in \mathbb{N}\}$. Como $1 - 1 = 0$, tenemos que $1 \in E$. Considere $m \in E$, entonces $m - 1 = 0$ ó $m - 1 \in \mathbb{N}$. En el primer caso tenemos $(m-1)+1 = 0+1 = 1 \in \mathbb{N}$, pero $(m - 1) + 1 = (m + 1) - 1$, entonces $(m + 1) - 1 \in \mathbb{N}$. En el segundo caso $m - 1 \in \mathbb{N}$ implica $(m - 1) + 1 \in \mathbb{N}$, por definición de $\mathbb{N}$. Luego en ambos casos $(m + 1) - 1 \in \mathbb{N}$, lo cual muestra que $m + 1 \in E$. Lo que prueba que E es inductivo.

(*iv*) Sea $n \in \mathbb{Z}$ tal que $n > 0$. Por definición de $\mathbb{Z}$ se tiene que $n = 0, n \in \mathbb{N}$ ó $-n \in \mathbb{N}$. Como $n > 0$, entonces $n \in \mathbb{N}$ ó $-n \in \mathbb{N}$. Si $-n \in \mathbb{N} \subseteq F^+$ tenemos que $-n > 0$, es decir $n < 0$, lo cual es absurdo, por tanto $n \in \mathbb{N}$.

(*v*) Pueden ocurrir tres casos. Caso 1: $p \in \mathbb{N}$. Defina $A := \{k \in \mathbb{N} : k - 1 \in \mathbb{Z}\}$. Claramente $1 \in A$. Si $k \in A$, entonces $(k+1) - 1 = k \in \mathbb{N} \subseteq \mathbb{Z}$, luego $k+1 \in A$ y asi A es inductivo. Como $p \in \mathbb{N}$ y $\mathbb{N} \subset A$, entonces $p \in A$, por tanto $p - 1 \in \mathbb{Z}$.
Caso 2: $-p \in \mathbb{N}$. Como $-(p - 1) = 1 - p = 1 + (-p) \in \mathbb{N}$, tenemos que $p - 1 \in \mathbb{Z}$.
Caso 3: $p = 0$. En este caso, $p - 1 = 0 - 1 = -1 \in \mathbb{Z}$. En cualquier caso tenemos la conclusión deseada.

(*vi*) En virtud de (*ii*) y (*iv*) es suficiente probar que $n - m \in \mathbb{Z}$. Para eso considere $n \in \mathbb{N}$ fijo y defina $B := \{k \in \mathbb{N} : n - k \in \mathbb{Z}\}$. Es claro que $1 \in B$. Si $k \in B$, entonces $k \in \mathbb{N}$ y $n - k \in \mathbb{Z}$, luego por (*v*) se tiene que $n - k - 1 \in \mathbb{Z}$, es decir, $n - (k + 1) \in \mathbb{Z}$. Asi $k + 1 \in B$. Por lo tanto B es inductivo. Como $m \in \mathbb{N}$ y $\mathbb{N} \subseteq B$, entonces $n - m \in \mathbb{Z}$. Lo cual termina la prueba. □

Teorema 6.33. *Si* m *y* n *son elementos naturales, también lo son* $m + n$ *y* mn.

Prueba: Fijemos $m \in \mathbb{N}$ y defina $E := \{k \in \mathbb{N} : m + k \in \mathbb{N}\}$. Como $m \in \mathbb{N}$ y $\mathbb{N}$ es un conjunto inductivo, entonces $m+1 \in \mathbb{N}$, lo cual significa que $1 \in E$. Supongamos que $k \in E$, luego $m+k \in \mathbb{N}$.

Nuevamente, usando el hecho que $\mathbb{N}$ inductivo se tiene que $(m+k)+1 \in \mathbb{N}$, entonces $m+(k+1) \in \mathbb{N}$, lo cual significa que $k+1 \in E$, lo que muestra que E es inductivo. La prueba de la segunda parte se deja al lector. □

La prueba del siguiente hecho será dejada al lector.

Proposición 6.34. *En un campo ordenado $m, n \in \mathbb{N}$ y $m > n$ implica $m - n \in \mathbb{N}$.*

El siguiente corolario nos dice que entre dos naturales consecutivos no puede haber otro natural, de hecho se puede probar que entre dos enteros consecutivos no existe otro entero, este hecho será dejado como ejercicio al lector.

Corolario 6.35. *Si $m < n < m+1$, entonces $n \notin \mathbb{N}$ o $m \notin \mathbb{N}$.*

Prueba: Suponga que $m, n \in \mathbb{N}$, entonces la hipótesis $n > m$ implica que $n - m \in \mathbb{N}$, luego $n - m \geq 1$ y por tanto $n \geq m+1$, lo cual contradice el hecho que $n < m+1$. Esto termina la prueba del corolario. □

A continuación demostraremos el denominado Principio del Buen orden (P. B. O.) Antes de establecer el P. B. O. daremos la definición de elemento mínimo de un subconjunto de un campo ordenado.

Definición 6.36 (Elemento Mínimo)**.** *Sean F un campo ordenado, $x \in F$ y $E \subseteq F$. Decimos que x es un elemento mínimo de E si $x \in E$ y $x \leq a$ para todo $a \in E$.*

Es fácil probar que un elemento mínimo cuando existe es único.

Teorema 6.37 (Principio de buen orden)**.** *En un campo ordenado, cualquier subconjunto E de $\mathbb{N}$ no vacío tiene un elemento mínimo*

Prueba: Consideremos el conjunto

$$A := \{a \in \mathbb{N} : a \leq e \text{ para todo } e \in E\}.$$

El conjunto A tiene las siguientes propiedades:
(i) $1 \in A$. Como $1 \in \mathbb{N}$, $1 \leq e$ para todo $e \in \mathbb{N}$ y $E \subseteq \mathbb{N}$, entonces $1 \leq e$ para todo $e \in E$. O sea que $1 \in A$.
(ii) Existe $x \in \mathbb{N}$ tal que $x \notin A$. (i.e., $A \neq \mathbb{N}$) Como E no es vacío podemos escoger $e_0 \in E$. Como $1 > 0$, tenemos que $1 + e_0 > e_0$ y por tanto $1 + e_0 \notin A$. Lo que prueba (ii). Ahora, usando (i) y (ii) podemos concluir que A no es inductivo y que existe $x_0 \in A$ tal que $x_0 + 1 \notin A$. Veamos que x_0 es elemento mínimo de E. En efecto, como $x_0 \in A$, entonces $x_0 \leq e$ para todo $e \in E$. Suponga que $x_0 \notin E$, entonces $x_0 < e$ para todo $e \in E$. Por Teorema 6.32 (v) tenemos que $x_0 + 1 \leq e$ para todo $e \in E$, es decir $x_0 + 1 \in A$, lo cual es absurdo. □

Teorema 6.38 (Segunda Ley de Inducción)**.** *Una proposición $p(n)$ vale para todo natural n en un campo ordenado si:*

(*i*) $p(1)$ *vale, y*

(*ii*) *si* $p(n)$ *vale para todos los naturales* n *menores que algún* $m \in \mathbb{N}$, $p(n)$ *también vale para* $n = m$.

Prueba: Razonemos por el absurdo. Supongamos que $p(n)$ falla para algún $n \in \mathbb{N}$ (llamenos a tal n "malo"). Definamos $A = \{k \in \mathbb{N} : p(k) \text{ falla}\}$. Por el Principio del Buen Orden A tiene un elemento mínimo. Sea tal mínimo m, entonces m es el menor natural para el cual $p(n)$ falla. Lo que significa que para todo natural n menor que m $p(n)$ es cierta (por (i) entre estos esta el 1). Pero entonces por la hipótesis (ii), $p(n)$ también vale para $n = m$, lo cual es imposible ya que m es "malo" por construcción. Esta contradicción muestra que no puede haber ningún $n \in \mathbb{N}$ malo, lo cual prueba el teorema. □

Nota 6.39. *En pruebas inductivas, el Teorema 6.31 se usa en muchas de ellas de la misma manera que el Teorema 6.38, pero éste deja más libertad en el paso* (ii). *En vez de asumir sólo que* $p(m)$ *es cierto, podemos asumir* $p(1)$, $p(2)$,...,$p(m-1)$ *son ciertos.*

Una ley de inducción similar aplica para deficiones: Un concepto $c(n)$ es mirado como definición para todo elemento natural de un campo ordenado F si

(*i*) ésta se ha definido para $n = 1$, y

(*ii*) alguna regla o formula se da de tal manera que expresa $c(n)$ en términos de $c(1), c(2), ..., c(n-1)$ i.e., en términos de $c(k)$ con $k < n$ o algunos de ellos.

Tales definiciones son llamadas inductivas o recursivas. La admisibilidad de las definiciones recursivas puedo probarse de la misma manera como se hizo para las pruebas inductivas. A continuación damos algunos ejemplos de definiciones recursivas:

Definición 6.40. *Dado un elemento* x *de un campo* F *y un número natural* $n \in \mathbb{R}$, *la* n*-ésima potencia de* x, *denotada* x^n, *se define como*

(*i*) $x^1 = x$ *y*

(*ii*) $x^{n+1} = x^n x$.

Si $x \neq 0$, *también se define* $x^0 = 1$ *y* $x^{-n} = (x^n)^{-1}$. *La expresión* 0^0 *permanece indefinida.*

Proposición 6.41. *Sea* F *un campo. Si* $a, b \in F$ *y* $m, n \in \mathbb{N} \subset \mathbb{R}$, *entonces*

(*i*) $a^m \cdot a^n = a^{m+n}$.

(*ii*) $(a^m)^n = a^{mn}$.

(*iii*) $(a \cdot b)^n = a^n \cdot b^n$.

Prueba: Ejercicio para el lector.

Definición 6.42. *Para todo número natural n, definimos recursivamente la expresión $n!$, lease n factorial, de la siguiente forma:*

(i) $1! = 1$

(ii) $n! = n \cdot (n-1)!$, *para* $n = 2, 3, 4, ...$

También se define $0! = 1$.

Definición 6.43. *La suma y el producto de n elementos $x_1, x_2, ..., x_n$ de un campo F, denotado por*

$$x_1 + x_2 + \cdots + x_n \quad y \quad x_1 \cdot x_2 \cdots x_n$$

(o $\sum_{k=1}^{n} x_k$ *y* $\prod_{k=1}^{n} x_k$, *respectivamente) son definidas recursivamente como:*

Sumas: (i) $\displaystyle\sum_{k=1}^{1} x_k = x_1$ (ii) $\displaystyle\sum_{k=1}^{n} x_k = \left(\sum_{k=1}^{n-1} x_k\right) + x_n,\ n = 2, 3, ...$

Productos: (i) $\displaystyle\prod_{k=1}^{1} x_k = x_1$ (ii) $\displaystyle\prod_{k=1}^{n} x_k = \left(\prod_{k=1}^{n-1} x_k\right) \cdot x_n,\ n = 2, 3, ...$

Nota 6.44. *Si $x_1 = x_2 = \cdots = x_n = x$ escribiremos nx por $\sum_{k=1}^{n} x_k$. Observe que aquí $n \in \mathbb{R}$, mientras que $x \in F$, entonces nx no es en general, el producto en F. Si $F \subseteq \mathbb{R}$, nx coincide con el producto ordinario en $\mathbb{R}$.*

Definición 6.45 (n-tupla)**.** *Para cualesquiera objetos $x_1, x_2, ..., x_n$ la n-tupla ordenada $(x_1, x_2, ..., x_n)$ se define como:*

(i) $(x_1) = x_1$

(ii) $(x_1, x_2, ..., x_n) = ((x_1, x_2, ..., x_{n-1}), x_n),\ n = 2, 3, ..$

También se puede definir el producto cartesiano

$$A_1 \times A_2 \times \cdots \times A_n$$

de n-conjuntos así

(i) $\displaystyle\prod_{k=1}^{1} A_k = A_1,\ y$

(ii) $\displaystyle\prod_{k=1}^{n} A_k = \left(\prod_{k=1}^{n-1} A_k\right) \times A_n,\ n = 2, 3, ...$

Definición 6.46. *Sean n, k enteros no negativos en $\mathbb{R}$, con $k \leq n$, definimos los coeficientes binomiales $\binom{n}{k}$ por*

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

Teorema 6.47. *Sean n, k números naturales tales que $1 \leq k \leq n$. Entonces*

(i) $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$

(i) $\binom{n}{k} \in \mathbb{N}$

Prueba:

(i)

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} =& \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} \\ =& \frac{n!k}{(n-k+1)!k!} + \frac{n!(n-k+1)}{(n-k+1)!k!} = \frac{n!(n+1)}{(n-k+1)!k!} \\ =& \frac{(n+1)!}{(n-k+1)!k!} = \frac{(n+1)!}{(n+1-k)!k!} = \binom{n+1}{k}\end{aligned}$$

(ii) Definamos $E = \{n \in \mathbb{N} : \binom{n}{k} \in \mathbb{N} \text{ para todo } k \in \mathbb{N},\ 1 \leq k \leq n\}$. Veamos que E es inductivo. En efecto, como $\binom{1}{1} = \frac{1!}{(1-1)!1!} = 1 \in \mathbb{N}$, entonces $1 \in E$. Supongamos que $\binom{m}{k} \in \mathbb{N}$ para todo $k \in \mathbb{N}$ con $1 \leq k \leq m$. Sea $k \in \mathbb{N}$ tal que $1 < k < m+1$, entonces $\binom{m+1}{k} = \binom{m}{k-1} + \binom{m}{k}$. Como $1 \leq k-1 \leq m$ y $1 < k \leq m$, por hipótesis inductiva $\binom{m}{k-1}, \binom{m}{k} \in \mathbb{N}$, por propiedad clausurativa de $\mathbb{N}$ probada en el Teorema 6.33 se tiene que $\binom{m+1}{k} \in \mathbb{N}$ para $1 < k < m+1$. Si $k = 1$ ó $k = m+1$, entonces $\binom{m+1}{k} = m+1$ ó $\binom{m+1}{k} = 1$, en cualquier caso $\binom{m+1}{k} \in \mathbb{N}$. Así que E es inductivo lo cual prueba que $E = \mathbb{N}$. □

Teorema 6.48. *Sean $a, b \in \mathbb{R} \setminus \{0\}$ y n un número natural. Entonces*

(i) $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ *(Fórmula Binomial)*

(ii) $a^n - b^n = (a-b) \sum_{k=1}^{n} a^{n-k} b^{k-1}$

Prueba:

(*i*) Sea $E := \{n \in \mathbb{N} : (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k\}$. Como $\binom{1}{0} = 1 = \binom{1}{1}$ y $a^0 = b^0 = 1$, entonces $(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^{1-k}b^k$, es decir $1 \in E$. Supongamos que $m \in E$, luego $(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k}b^k$. Entonces

$$\begin{aligned}
(a+b)^{m+1} =& (a+b)(a+b)^m = (a+b)\sum_{k=0}^{m}\binom{m}{k}a^{m-k}b^k \\
=& \sum_{k=0}^{m}\binom{m}{k}a^{m-k+1}b^k + \sum_{k=0}^{m}\binom{m}{k}a^{m-k}b^{k+1} \\
=& a^{m+1} + \sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k + \sum_{k=0}^{m-1}\binom{m}{k}a^{m-k}b^{k+1} + b^{m+1} \\
=& a^{m+1} + \sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k + \sum_{k=1}^{m}\binom{m}{k-1}a^{m-k+1}b^k + b^{m+1} \\
=& a^{m+1} + \sum_{k=1}^{m} a^{m-k+1}b^k\left[\binom{m}{k} + \binom{m}{k-1}\right] + b^{m+1} \\
=& a^{m+1} + \sum_{k=1}^{m}\binom{m+1}{k}a^{m-k+1}b^k + b^{m+1} = \sum_{k=0}^{m+1}\binom{m+1}{k}a^{m-k+1}b^k.
\end{aligned}$$

Por lo tanto $m+1 \in E$, lo que prueba que E es inductivo, así que $E = \mathbb{N}$.

(*ii*)

$$\begin{aligned}
(a-b)\sum_{k=1}^{n} a^{n-k}b^{k-1} =& \sum_{k=1}^{n} a^{n-k+1}b^{k-1} - \sum_{k=1}^{n} a^{n-k}b^k \\
=& a^n + \sum_{k=2}^{n} a^{n-k+1}b^{k-1} - \sum_{k=1}^{n-1} a^{n-k}b^k - b^n \\
=& a^n + \sum_{k=1}^{n-1} a^{n-k}b^k - \sum_{k=1}^{n-1} a^{n-k}b^k - b^n = a^n - b^n.
\end{aligned}$$

□

A continuación demostraremos algunas desigualdades importantes

Ejemplo 6.49. *Si* $a_1, a_2, ..., a_n \in \mathbb{R}^+$ *y* $a_1a_2\cdots a_n = 1$, *entonces* $a_1 + a_2 + \cdots + a_n \geq n$.

Prueba: Sea $E = \{n \in \mathbb{N} : a_1a_2\cdots a_n = 1 \Rightarrow a_1 + a_2 + \cdots + a_n \geq n\}$. Si $n = 1$, entonces $a_1 = 1$ por tanto $a_1 \geq 1$. Luego $1 \in E$. Ahora, supongamos que $k \in E$ entonces $a_1a_2\cdots a_k = 1$ implica $a_1 + a_2 + \cdots + a_k \geq k$. Veamos que $k+1 \in E$. Para eso supongamos que $a_1a_2\cdots a_ka_{k+1} = 1$. Consideraremos dos casos:
Caso 1: Si $a_1{=}a_2{=}\cdots = a_k{=}a_{k+1} = 1$. Claramente $a_1{+}\cdots{+}a_k + a_{k+1} = k+1$ luego $k+1 \in E$.

Caso 2: Existe $a_j \neq 1$. Sin perdida de generalidad supongamos que $a_j > 1$. Si $a_i > 1$ para todo $i = 1, 2, ...j-1, j+1, ...k+1$ entonces $a_1 \cdots a_k a_{k+1} > 1$, lo cual es absurdo, entonces existe $a_i < 1$. De nuevo sin perdida de generalidad suponga que $a_k > 1$ y $a_{k+1} < 1$. Como $a_1 \cdots a_k a_{k+1} = 1$, por hipótesis inductiva $a_1 + a_2 + \cdots + a_k a_{k+1} \geq k$, luego

$$a_1 + a_2 + \cdots + a_k + a_{k+1} \geq k - a_k a_{k+1} + a_k + a_{k+1}$$

Como $a_k > 1$ y $a_{k+1} < 1$, se tiene que $(a_{k+1} - 1)(1 - a_k) \geq 0$, así $a_{k+1} - a_k a_{k+1} - 1 + a_k \geq 0$. Lo que implica que $k - a_k a_{k+1} + a_k + a_{k+1} \geq k + 1$. Por tanto

$$a_1 + a_2 + \cdots + a_k + a_{k+1} \geq k + 1,$$

entonces $k + 1 \in E$. Lo que prueba que E es inductivo. □

Ejemplo 6.50. *Denote A_n, G_n y H_n la media Aritmética, Geométrica y Armónica, respectivamente, de n números reales positivos $a_1, a_2, ..., a_n$. Mas especificamente,*

$$A_n = \frac{a_1 + a_2 + ... + a_n}{n}, \quad G_n = \sqrt[n]{a_1 a_2 \cdots a_n} \quad y \quad H_n = \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + ... + \frac{1}{a_n}} \cdot$$

Muestre que $H_n \leq G_n \leq A_n$.

Prueba: Definamos $x_k = \frac{a_k}{\sqrt[n]{a_1 a_2 \cdots a_n}}$, para $k = 1, 2, .., n$. Note que $x_1 x_2 \cdots x_n = 1$, por el ejemplo anterior tenemos que $x_1 + x_2 + \cdots + x_n \geq n$. Luego

$$\frac{a_1}{\sqrt[n]{a_1 a_2 \cdots a_n}} + \frac{a_2}{\sqrt[n]{a_1 a_2 \cdots a_n}} + \cdots + \frac{a_n}{\sqrt[n]{a_1 a_2 \cdots a_n}} \geq n$$

Despejando obtenemos

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}$$

Luego $A_n \geq G_n$. Para la otra desigualdad, definamos $x_j = \frac{\sqrt[n]{a_1 a_2 \cdots a_n}}{a_j}$. Note que $x_1 . x_2 ... x_n = 1$, luego por ejemplo anterior tenemos que $x_1 + x_2 + ... + x_n \geq n$. Es decir

$$\sqrt[n]{a_1 . a_2 ... a_n} \left(\frac{1}{a_1} + \frac{1}{a_2} + ... + \frac{1}{a_n} \right) \geq n$$

despejando obtenemos

$$\sqrt[n]{a_1 a_2 \cdots a_n} \geq \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}}.$$

Por tanto $G_n \geq H_n$. Lo que muestra el resultado deseado. □

6.5. Enteros y Racionales.

La definición de los números enteros en un campo F fue dada anteriormente, en esta sección establecemos algunas propiedades adicionales de los números enteros y definimos los número racionales. Los tres primeros resultados son dejados como ejercicio al lector.

Lema 6.51. *Si $m, n \in \mathbb{N}$ en un campo F, entonces $m - n \in \mathbb{Z}$.*

Teorema 6.52. *Si x, y son enteros en un campo F, entonces $x + y$ y $x \cdot y$ también son enteros.*

Definición 6.53. *Sea x un elemento de un campo F con $x \neq 0$. Considere $m \in \mathbb{Z}$ con $m < 0$. Definimos x^m como*

$$x^m := \frac{1}{x^{-m}}.$$

Proposición 6.54. *Sea F un campo. Si $a, b \in F^+$ y $m, n \in \mathbb{Z}$, entonces*

(*i*) $a^m \cdot a^n = a^{m+n}$.

(*ii*) $(a^m)^n = a^{mn}$.

(*iii*) $(a \cdot b)^n = a^n \cdot b^n$.

Ley de inducción para enteros: Sea p un entero fijo, una proposición $P(n)$ vale para todo entero $n > p$, en un campo ordenado si

(i') $P(n)$ vale para $n = p + 1$.

(ii') $P(n)$ vale para todos los entero n tal que $p < n < m$, entonces $P(n)$ también vale para $n = m$ ($m \in \mathbb{Z}$).

Esta ley de inducción se prueba usando el Teorema 6.31 tomando $n = x - p$ y notando que $x - p$ se mueve a través de todos los naturales cuando $x > p$ y $x \in \mathbb{Z}$.

Definición 6.55 (Racionales)**.** *Un elemento x de un campo F se dice racional si $x = p/q$ para algunos $p \in \mathbb{Z}$ y $q \in \mathbb{N}$. Al conjunto de racionales lo notaremos $\mathbb{Q}$. En símbolos sería:*

$$\mathbb{Q} := \{p \cdot q^{-1} : p \in \mathbb{Z} \quad y \quad q \in \mathbb{N}\}.$$

Es claro de las definiciones hasta aquí dadas que

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subseteq \mathbb{R}.$$

A continuacion introducimos algunas leyes de composición interna de los números racionales y su prueba es dejada como ejercicio al lector.

Teorema 6.56. *La suma, diferencia y el producto de dos elementos racionales x e y en un campo F, también son racionales. Si además $y \neq 0$, entonces x/y es racional. De hecho $\mathbb{Q}$ es un campo ordenado.*

A continuación presentamos un ejemplo donde se usa el Teorema 6.38 o la Segunda Ley de Inducción.

Ejemplo 6.57. *Para todo entero positivo n, muestre que*

$$\frac{(1+\sqrt{5})^n-(1-\sqrt{5})^n}{2^n\sqrt{5}}$$

es un entero positivo.

Prueba: Definamos $\alpha := 1+\sqrt{5}$ y $\beta := 1-\sqrt{5}$. Es fácil ver que α y β son irracionales; además $\alpha+\beta=2$, $\alpha-\beta=2\sqrt{5}$ y $\alpha\beta=-4$. Considere el siguiente conjunto

$$E=\left\{n\in\mathbb{N}:\frac{\alpha^n-\beta^n}{2^n\sqrt{5}}\in\mathbb{N}\right\}.$$

Como $\frac{\alpha-\beta}{2\sqrt{5}}=1$, se tiene que $1\in E$. Asumamos que $n\in E$ y probaremos que $n+1\in E$. Note que

$$\begin{aligned}\frac{\alpha^{n+1}-\beta^{n+1}}{2^{n+1}\sqrt{5}}&=\frac{\alpha^n+\sqrt{5}\alpha^n-\beta^n+\sqrt{5}\beta^n}{2^{n+1}\sqrt{5}}=\frac{2\alpha^n-2\beta^n-\alpha^n+\beta^n+\sqrt{5}\alpha^n+\sqrt{5}\beta^n}{2^{n+1}\sqrt{5}}\\&=\frac{\alpha^n-\beta^n}{2^n\sqrt{5}}+\frac{(1+\sqrt{5})\beta^n-(1-\sqrt{5})\alpha^n}{2^{n+1}\sqrt{5}}=\frac{\alpha^n-\beta^n}{2^n\sqrt{5}}+\frac{\alpha\beta\beta^{n-1}-\alpha\beta\alpha^{n-1}}{2^{n+1}\sqrt{5}}\\&=\frac{\alpha^n-\beta^n}{2^n\sqrt{5}}+\frac{4\alpha^{n-1}-4\beta^{n-1}}{2^{n+1}\sqrt{5}}=\frac{\alpha^n-\beta^n}{2^n\sqrt{5}}+\frac{\alpha^{n-1}-\beta^{n-1}}{2^{n-1}\sqrt{5}}\end{aligned}$$

Luego

$$\frac{\alpha^{n+1}-\beta^{n+1}}{2^{n+1}\sqrt{5}}=\frac{\alpha^n-\beta^n}{2^n\sqrt{5}}+\frac{\alpha^{n-1}-\beta^{n-1}}{2^{n-1}\sqrt{5}}. \tag{6.5}$$

Como $n, n-1\in E$, se concluye que $\frac{\alpha^n-\beta^n}{2^n\sqrt{5}}$ y $\frac{\alpha^{n-1}-\beta^{n-1}}{2^{n-1}\sqrt{5}}$ son enteros positivos y por tanto su suma también lo es, usando (6.5) se obtiene que $\frac{\alpha^{n+1}-\beta^{n+1}}{2^{n+1}\sqrt{5}}$ es un entero y positivo. Así que $n+1\in E$, lo que concluye la prueba. □

6.6. Ejercicios

1. Sean $a,b,c,d\in\mathbb{R}$. Probar que:

 a) $(-a)\cdot(-b)=a\cdot b$.

 b) $(a-b)c=ac-bc$

 c) $ab=0$ si y sólo si $a=0$ o $b=0$.

 d) Si $a\neq 0$, entonces $(a^{-1})^{-1}=a$.

 e) Si $a\cdot b\neq 0$, entonces $(a\cdot b)^{-1}=a^{-1}\cdot b^{-1}$.

 f) Si $b\cdot d\neq 0$, entonces

 $$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}\quad\text{y}\quad\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}.$$

2. Sean $a, b \in \mathbb{R}$. Muestre que

 a) Si $a < 0$, entonces $a^{-1} < 0$.

 b) Si $a < 0 < b$, entonces $a^{-1} < b^{-1}$.

 c) Si $ab > 0$, entonces $(a > 0 \wedge b > 0) \ \vee \ (a < 0 \wedge b < 0)$.

 d) Si $ab < 0$, entonces $(a > 0 \wedge b < 0) \ \vee \ (a < 0 \wedge b > 0)$.

 e) Si $a^2 = a$, entonces $a = 0$ ó $a = 1$.

3. Utilice el Principio de Buen Orden para demostrar el Principio de Inducción Matemática.

4. Dar ejemplos de conjuntos inductivos diferentes de $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$.

5. Sean $a, b \in \mathbb{R}$ tales que $ab \neq 0$ y $m, n \in \mathbb{Z}$. Probar que :

 a) $a^m a^n = a^{m+n}$.

 b) $(a^m)^n = a^{mn}$.

 c) $(ab)^n = a^n b^n$.

6. Sean $a, b \in \mathbb{R}$ tales que $a^2 + b^2 = 1$. Probar que $|a + b| \leq \sqrt{2}$.

7. *a*) Si $a, b \in \mathbb{R}$, muestre que $2ab \leq a^2 + b^2$ y $4ab \leq (a + b)^2$. Pruebe que una condición necesaria y suficiente para la igualdad es que $a = b$.

 b) Sean $a, b \in \mathbb{R}^+$ tales que $a + b = 1$. Probar que:

 $$\left(a + \frac{1}{a}\right)^2 + \left(b + \frac{1}{b}\right)^2 \geq \frac{25}{2}.$$

 ¿Cuándo se obtiene la igualdad?

8. *Desigualdades de Bernoulli*: Sea $n \in \mathbb{N}$. Probar que para todo $x > -1$:

 a) $(1 + x)^n \geq 1 + nx$.

 b) $(1 + x)^n \geq 1 + nx + \frac{1}{2}n(n - 1)x^2$.

9. Sean $x \geq 0$ y n un entero positivo. Muestre que $x^{n+1} - (n + 1)x + n \geq 0$.

10. Sean x un número real y n un entero positivo. Muestre que $(1 - x^2)^n \geq 1 - nx^2$.

11. *a*) Si $a_1, a_2, \ldots, a_n \in \mathbb{R}^+$, muestre que

 $$(a_1 + a_2 + \cdots + a_n)\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}\right) \geq n^2.$$

 b) Si $a, b, c \in \mathbb{R}^+$ y $a + b + c = 1$, muestre que

 $$\left(\frac{1}{a} - 1\right)\left(\frac{1}{b} - 1\right)\left(\frac{1}{c} - 1\right) \geq 8.$$

12. Sean a_k, b_k con $k = 1, 2, \ldots, n$ números reales. Muestre que

a)
$$\left(\sum_{k=1}^{n} a_k b_k\right)^2 \leq \sum_{k=1}^{n} a_k^2 \sum_{k=1}^{n} b_k^2.$$

b)
$$\left(\sum_{k=1}^{n} (a_k + b_k)^2\right)^{1/2} \leq \left(\sum_{k=1}^{n} a_k^2\right)^{1/2} + \left(\sum_{k=1}^{n} b_k^2\right)^{1/2}.$$

c)
$$\sum_{k=1}^{n} a_k \sum_{k=1}^{n} \frac{1 - a_k}{a_k} \geq n \sum_{k=1}^{n} (1 - a_k).$$

13. Sean $a_1, a_2, \ldots, a_n \in \mathbb{R}^+ \cup \{0\}$ tales que $a_1 + a_2 + \cdots + a_n \leq \frac{1}{2}$. Probar que
$$(1 - a_1)(1 - a_2) \cdots (1 - a_n) \geq \frac{1}{2}.$$

14. Si $a_1, a_2, \ldots, a_n \in \mathbb{R}^+$ y $a_1 a_2 \cdots a_n = 1$, muestre que
$$(1 + a_1)(1 + a_2) \cdots (1 + a_n) \geq 2^n.$$

15. Pruebe que si $n \in \mathbb{N}$, entonces $n! \leq \left(\frac{n+1}{2}\right)^n$.

16. Pruebe que si $n \in \mathbb{N}$, entonces $(2n)! \leq 4^n (n!)^2$.

17. Muestre que:

a) $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

b) $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

c) $\sum_{k=1}^{n} k^3 = \left[\frac{n(n+1)}{2}\right]^2$.

d) $\sum_{k=1}^{n} k^4 = \frac{6n^5+15n^4+10n^3-n}{30}$.

18. Sean $a, b, c \in \mathbb{R}^+$. Probar que:

a) $\frac{bc}{a} + \frac{ac}{b} + \frac{ab}{c} \geq a + b + c$.

b) $\frac{a^3 + b^3 + c^3}{a^2 + b^2 + c^2} \geq \frac{a + b + c}{3}$.

c) $(a + b)^2 \leq (1 + c)a^2 + \left(1 + \frac{1}{c}\right) b^2$.

19. Muestre que $n^3 + 5n$ es divisible por 6, para todo natural n.

20. Muestre que $\frac{4^n - 1}{3}$ es un entero, si n es un entero positivo.

21. Sean $x \neq 1$ un número real y n un número natural. Muestre que:

a) $1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}$.

b) $1 + 2x + 3x^2 + \cdots + nx^{n-1} = \frac{nx^n}{x-1} - \frac{x^n-1}{(x-1)^2}$.

22. Sean $a > 1$ un número real y n un número natural. Muestre que:

 a) $\frac{1+a+a^2+\cdots+a^{n-1}}{n} < \frac{1+a+a^2+\cdots+a^n}{n+1}$.

 b) $\frac{a^n-1}{n} < \frac{a^{n+1}-1}{n+1}$.

23. Encuentre todos lo naturales n tales que $n^2 < 2^n$.

24. Sea n un natural, muestre que $1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \geq \sqrt{n}$.

25. Sean m un entero y n un número real tal que $m < n < m + 1$. Muestre que n no es un entero.

26. Sea $a \neq 1$ un número real. Pruebe que $\prod_{k=0}^{n} (1 + a^{2k}) = \dfrac{1 - a^{2n+1}}{1 - a}$.

27. Sea $n \geq 2$ un entero. Muestre que

$$\prod_{k=0}^{n} \binom{n}{k} \leq \left(\frac{2^n - 2}{n - 1} \right)^{n-1}.$$

28. Intente mostrar por inducción que $\frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 1$, para todo entero $n \geq 2$. Después de un tiempo se dará cuenta que es algo difícil, sin embargo se puede probar una desigualdad parecida que demostraría la anterior. Para lograr este cometido, muestre que $\frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 1 - \frac{1}{n}$ para todo entero $n \geq 2$. Note que esta última desigualdad si se puede hacer por inducción.

Capítulo 7

Conjuntos Acotados en un Campo Ordenado.

Hasta ahora las propiedades algebraicas que hemos estudiado nos permiten diferenciar de manera clara a los números reales de los naturales y los enteros, pero no es clara la diferencia con los racionales. Como ya habrá notado todo campo ordenado es infinito y tiene la propiedad que entre dos elementos distintos siempre hay tercero, lo cual es común para los reales y los racionales, lo que implica que en estos campos los números están tan cerca como se desee. La propiedad fundamental que distingue el conjunto de los números reales de los racionales es el Axioma de Completez (o Axioma de la Mínima Cota Superior), en este capítulo introducimos tal axioma y con esto completamos el estudio de las propiedades de los números reales. Probaremos la propiedad Arquimediana de los reales, la existencia de raíces y todas las propiedades de la potenciación que conocemos. Comenzaremos con algunas definiciones.

Definición 7.1 (Cotas inferior y superior)**.** *Un subconjunto A de un campo ordenado F se dice acotado inferiormente, si existe un elemento $p \in F$ tal que $p \leq x$ para todo $x \in A$. El conjunto A es acotado superiormente, si existe un elemento $q \in F$ tal que $x \leq q$ para todo $x \in A$. En este caso, p y q son llamados, respectivamente, una cota inferior y una cota superior de A. Si A es acotado superiormente e inferiormente al mismo tiempo, diremos que A es acotado (por p y q). El conjunto vacío $\varnothing$ es acotado y todos los elementos de F son considerados cotas inferiores y superiores.*

Nota 7.2. *Las cotas p y q de la definición anterior pueden no pertenecer a A.*

Daremos algunos ejemplos de conjuntos acotados y no acotados, las pruebas rigurosas de estos hechos serán dadas más adelante.

(1) El conjunto $\{1, -2, 3, 7\}$ es acotado superiormente e inferiormente. Superiormente, por ejemplo, por 7, 100,... e inferiormente, por ejemplo por, $-2, -3, -10$,...

(2) El conjunto de los números naturales $\mathbb{N} = \{1, 2, 3, ...\}$ es acotado inferiormente (ejemplo por $1, 0, -\frac{1}{2}$,..) pero no superiormente.

(3) $\mathbb{Z}$ no es acotado superiormente y tampoco inferiormente.

Definición 7.3. *Dados números a y b ($a \leq b$), definimos*

(*i*) *El intervalo abierto (a, b) por*

$$(a, b) := \{x \in \mathbb{R} : a < x < b\}$$

(*ii*) *El intervalo cerrado $[a, b]$ como*

$$[a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}$$

(*iii*) *El intervalo semi-abierto $(a, b]$ por*

$$(a, b] := \{x \in \mathbb{R} : a < x \leq b\}$$

(*iv*) *El intervalo semi-cerrado $[a, b)$ como*

$$[a, b) := \{x \in \mathbb{R} : a \leq x < b\}.$$

Si $a = b$, decimos que el intervalo es degenerado, en cuyo caso

$$[a, a] = \{a\}, \quad (a, a] = (a, a) = [a, a) = \varnothing.$$

Definición 7.4 (Supremo)**.** *Un número s es llamado un supremo del conjunto A si*

(*i*) *s es una cota superior de A.*

(*ii*) *Si $m \in \mathbb{R}$ y m es una cota superior de A, entonces $s \leq m$.*

Nótese que de (ii) tenemos que un supremo, cuando existe, es la menor de las cotas superiores de A.

Definición 7.5 (Ínfimo)**.** *Un número t es llamado un ínfimo del conjunto A si*

(*i*) *t es una cota inferior de A.*

(*ii*) *Si $m \in \mathbb{R}$ y m es una cota inferior de A, entonces $m \leq t$.*

Proposición 7.6. *Un subconjunto A de $\mathbb{R}$ tiene a lo más un supremo (ínfimo).*

Prueba: Sean s_1 y s_2 supremos de A, entonces s_1 y s_2 son cotas superiores de A, en virtud de (ii) se tiene que $s_1 \leq s_2$ y $s_2 \leq s_1$, por tanto $s_1 = s_2$. □

La proposición anterior muestra que si A tiene un supremo (ínfimo), éste es único y por tanto podemos hablar de "el" supremo (respectivamente "el" ínfimo). En tal caso lo denotaremos $\sup A$ (respectivamente $\inf A$).

Proposición 7.7. *Si un subconjunto de $\mathbb{R}$ tiene una cota superior, entonces tiene infinitas cotas superiores.*

Definición 7.8. *Un número M es llamado un máximo del conjunto $A \subset \mathbb{R}$ si M es una cota superior de A y $M \in A$. Si $A \subset \mathbb{R}$ tiene un máximo, éste es único por lo tanto podemos hablar del "el" máximo, lo notaremos* $\max A$.
De igual manera decimos que un número m es un mínimo de A si m es una cota inferior de A y $m \in A$. En este caso también m es único, luego podemos hablar del mínimo, y lo notaremos $\min A$.

Axioma de Completez.
Si M es un conjunto no vacío de $\mathbb{R}$ acotado superiormente, entonces M tiene supremo (finito).

No se necesita ningún axioma para cotas inferiores, ya que la correspondiente proposición puede ser probada usando el axioma de completez.

Teorema 7.9. *Si M es un subconjunto no vacío de números reales acotado inferiormente, entonces M tiene ínfimo (finito).*

Prueba: Sea $B := \{q \in \mathbb{R} : q$ cota inferior para M$\}$, $B \neq \varnothing$ ya que M es acotado inferior. Claramente cualquier elemento de M ($M \neq \varnothing$) es cota superior para B. Entonces B es un subconjunto de $\mathbb{R}$, no vacío y acotado superiormente. Así por el Axioma de Completez B tiene un supremo (finito), que llamaremos p. Probaremos que p es el infimo de M. En efecto:

(*i*) Suponga que existe un $x_0 \in M$ tal que $p > x_0$. Luego por definición de B tenemos que $x_0 \geq b$ para todo $b \in B$. Así que x_0 es cota superior para B, por tanto $p \leq x_0$, lo cual es absurdo.

(*ii*) Considere m una cota inferior para M, entonces $m \in B$ y por tanto $p \geq m$. □

Vale la pena notar que el teorema anterior pudo ser tomado como un axioma y el Axioma de Completez deducido de él.

Definición 7.10 (Campo Ordenado Completo)**.** *Un campo ordenado F se dice completo (o Arquimediano) si todo subconjunto M de F no vacío acotado superiormente tiene un supremo en F.*

En particular $\mathbb{R}$ es completo.

Teorema 7.11. *En un campo ordenado completo F, todo subconjunto de F acotado inferiormente y no vacío, tiene un ínfimo en F.*

Corolario 7.12 (Propiedad de Aproximación del Supremo)**.** *Sean $E \subset \mathbb{R}$ y $s \in \mathbb{R}$, entonces $s =$* $\sup E$ *si y sólo si*

(*i*) *s es una cota superior de E y*

(*ii*) *para todo $\epsilon > 0$, existe $a \in E$ tal que $s - \epsilon < a$.*

Prueba: " $\Rightarrow$ " Si $s = \sup E$, entonces por definición s es una cota superior para E. Ahora bien, supongamos, por el absurdo, que existe $\epsilon_0 > 0$ tal que para todo $a \in E$ se tiene que $a \leq s - \epsilon_0$, luego $s - \epsilon_0$ es una cota superior para E, por tanto, $s \leq s - \epsilon_0$ lo cual es absurdo.
" $\Leftarrow$ " Por hipótesis ya tenemos que s es una cota superior para E, veamos que es la mínima. Sea $M \in \mathbb{R}$ una cota superior para E y $\epsilon > 0$. De nuevo por hipótesis existe $a \in E$ tal que $s - \epsilon < a$, pero $a \leq M$, entonces $s < \epsilon + a \leq M + \epsilon$, para todo $\epsilon > 0$. Por tanto $s \leq M$, lo cual implica que $s = \sup E$. □

Corolario 7.13. *Si A y B son subconjuntos no vacíos de un campo ordenado F y $A \subseteq B$, entonces*

$$\sup A \leq \sup B \quad e \quad \text{ínf}\, B \leq \text{ínf}\, A,$$

provisto de que los ínfimos y supremos anteriores existan.

Prueba: Sean $p = \sup A$ y $q = \sup B$. Como q es una cota superior para B, tenemos que $x \leq q$ para todo $x \in B$. Pero $A \subseteq B$, entonces $x \leq q$ para todo $x \in A$, por tanto $\sup A = p \leq q = \sup B$. En forma similar se prueba la otra desigualdad. □

Corolario 7.14. *Si un subconjunto M de un campo ordenado F tiene máximo q, entonces q es también su supremo. Similarmente, el mínimo de M es también su infimo (provisto que estos mínimos y máximos existan).*

Teorema 7.15. *$\mathbb{Z}$ no es acotado superiormente.*

Prueba: Razonemos por el absurdo, es decir, supongamos que $\mathbb{Z}$ es acotado superiormente. Por el axioma de completez existe $s \in \mathbb{R}$ tal que $s = \sup \mathbb{Z}$. Por la propiedad de aproximación al supremo existe $m \in \mathbb{Z}$ tal que $s - 1 < m$, i.e., $s < m + 1$ y $m + 1 \in \mathbb{Z}$, lo cual contradice el hecho que $s = \sup \mathbb{Z}$. □

7.1. Aplicaciones del Axioma de Completez.

Teorema 7.16 (Propiedad Arquimediana)**.** *Sean $x, y \in F$, donde F es un campo ordenado completo y $x > 0$, entonces existe $n \in \mathbb{N}$ tal que $nx > y$.*

Prueba: Razonemos por el absurdo. Dado $x > 0$ supongamos que para todo natural n, tenemos $nx \leq y$. Definamos

$$M = \{nx : n \in \mathbb{N}\}.$$

Claramente $M \neq \varnothing$ y es acotado superiormente por y. Por la completez de F, M tiene un supremo, que denotamos q. Como q es cota superior de M, entonces $nx \leq q$ para todo natural $n \in F$. Pero si n es natural, $n + 1$ también es un natural de F. Luego $(n + 1)x \leq q$, así $nx \leq q - x$, para todo n natural de F, lo cual indica que $q - x$ es una cota superior para M, como $q = \sup M$, entonces $q \leq q - x$, por tanto $0 \leq -x$ lo cual es absurdo, ya que $x > 0$. □

Nota 7.17. *Si hacemos $x = \epsilon$ y $y = 1$ en el teorema anterior, tenemos que para todo $\epsilon > 0$ existe $n \in \mathbb{N}$ tal que $\frac{1}{n} < \epsilon$, es decir existen racionales arbitrariamente pequeños.*

Corolario 7.18. *Dado un elemento y en un campo ordenado completo (Arquimediano) F, existen m, n naturales tales que $-m < y < n$.*

Prueba: Dados $y \in F$ y $x = 1$, por la Propiedad Arquimediana existe $n \in \mathbb{N}$ tal que $1 \cdot n > y$, i.e., $n > y$. Como $y \in F$, entonces $-y \in F$, luego por la Propiedad Arquimediana existe $m \in \mathbb{N}$ tal que $1 \cdot m > -y$, por tanto $-m < y < n$. □

Corolario 7.19. *En cualquier campo Arquimediano F, $\mathbb{N}$ no tiene cota superior y $\mathbb{Z}$ no tiene cota superior ni inferior.*

Teorema 7.20. *En cualquier campo Arquimediano F, todo subconjunto no vacío de enteros acotado superiormente tiene máximo, y todo subconjunto no vacío de enteros acotado inferiormente tiene mínimo.*

Prueba: Sea M un subconjunto de enteros no vacío y acotado superiormente en un campo completo F. Por el axioma de completez M tiene un supremo, al cual denotaremos q. Sólo debemos probar que $q \in M$. Razonemos por el absurdo, supongamos que $q \notin M$. Como $q - 1 < q$, por la propiedad de aproximación al supremo existe $x \in M$ tal que $q - 1 < x \leq q$, pero $x \neq q$ ya que $q \notin M$, luego $q - 1 < x < q$. Como $x < q$, podemos definir $\epsilon := q - x > 0$ y de nuevo por la propiedad de aproximación al supremo, existe $y \in M$ tal que $x = q - \epsilon < y \leq q$, y se tendría que $y \neq q$ pues $q \notin M$. Hasta aquí hemos probado que existen $x, y \in M$ tales que $q - 1 < x < y < q$. De la desigualdad anterior es muy fácil concluir que $0 < y - x < 1$, lo cual es absurdo ya que $x, y \in M \subseteq \mathbb{Z}$, lo que implica que $q \in M$. La prueba para el caso que M sea un subconjunto de enteros no vacío y acotado inferiormente es dejada como ejercicio al lector. □

Corolario 7.21. *Dado un elemento x en un campo arquimediano F, siempre existe un único entero $n \in F$, tal que*

$$n \leq x < n + 1.$$

Este entero es llamado parte entera de x y lo denotaremos como $\lfloor x \rfloor$.

Prueba: Sea $x \in F$. Tomemos $M = \{m \in \mathbb{Z} : m \leq x\}$, M es acotado superiormente y no vacío, por tanto M tiene un máximo, llamemoslo n, luego $n \leq x$. Como $n + 1 > n$, entonces $n + 1 \notin M$. Luego $x < n + 1$, entonces $n \leq x < n + 1$. Como n es un máximo n es único, lo que termina la prueba del corolario. □

Ejemplo 7.22.

$$\left\lfloor \frac{1}{2} \right\rfloor = 0, \quad \lfloor -11/4 \rfloor = -2, \quad \lfloor -4 \rfloor = -4, \quad \lfloor \sqrt{2} \rfloor = 1.$$

Teorema 7.23 (Densidad de los Racionales)**.** *Dados elementos a y b en un campo arquimediano F tales que $a < b$, siempre existe un racional $r \in F$ tal que $a < r < b$.*

Prueba: Como $b-a>0$, existe $n\in\mathbb{N}$ tal que $n(b-a)>1$, por tanto $\dfrac{1}{n}<b-a$. Como $na\in F$, existe que $m\in\mathbb{Z}$ tal que $m\leq na<m+1$, luego

$$a<\frac{m+1}{n}=\frac{m}{n}+\frac{1}{n}\leq a+\frac{1}{n}<b.$$

Defina $q=\dfrac{m+1}{n}$, note que $q\in\mathbb{Q}$ y cumple $a<q<b$. □

7.2. Algunos Resultados Adicionales

Definición 7.24. *Sean A y B subconjuntos no vacíos de $\mathbb{R}$. definamos*

$$\begin{aligned}-A :=&\{a : -a\in A\}\\ A+B :=&\{a+b : a\in A \text{ y } b\in B\}\\ A-B :=&A+(-B)\end{aligned}$$

Si $A,B\subset\mathbb{R}^+$, definimos

$$\begin{aligned}AB :=&\{ab : a\in A \text{ y } b\in B\}\\ \frac{1}{A} :=&\left\{\frac{1}{a} : a\in A\right\}\end{aligned}$$

Teorema 7.25. *Sea E un subconjunto no vacío de $\mathbb{R}$.*

(*i*) *E tiene supremo si y sólo si $-E$ tiene infimo. En tal caso*

$$\text{ínf}(-E)=-\sup E.$$

(*ii*) *E tiene ínfimo si y sólo si $-E$ tiene supremo. En tal caso*

$$\sup(-E)=-\,\text{ínf}\,E.$$

Prueba:

(*i*) " $\Rightarrow$ " Sean $s=\sup E$ y $t=-s$. Como $a\leq s$ para todo $a\in E$, entonces $-s\leq -a$, para todo $a\in E$, así que t es cota inferior para $-E$. Sea t_0 una cota inferior para $-E$, luego $t_0\leq -a$ para todo $a\in E$. Por tanto $a\leq -t_0$, para todo $a\in E$, lo que indica que $-t_0$ es una cota superior para E, entonces $s\leq -t_0$, es decir, $t\geq t_0$. En consecuencia $\text{ínf}(-E)=t=-\sup E$.
" $\Leftarrow$ " Como $-E$ esta acotado inferiormente, sea m una cota inferior de $-E$, i.e., $m\leq -a$ para todo $a\in E$, lo que indica que $-m$ es una cota superior de E, como $E\neq\varnothing$ y acotado superiormente E tiene supremo.

(*ii*) $-\,\text{ínf}\,E=-\,\text{ínf}(-(-E))=-(-\sup(-E))=\sup(-E)$. □

Teorema 7.26. *Sean A y B subconjuntos no vacíos de $\mathbb{R}$ acotados superiormente, entonces*

$$\sup(A+B) = \sup A + \sup B.$$

Prueba: Claramente $A+B \neq \varnothing$. Sea $z \in A+B$, entonces existen $a \in A$ y $b \in B$ tales que $z = a+b$. Como $a \leq \sup A$ y $b \leq \sup B$, entonces

$$a+b \leq \sup A + \sup B.$$

Lo que implica que $\sup A + \sup B$ es una cota superior para $A+B$. Ahora, considere $\epsilon > 0$, por la propiedad de aproximación del supremo existe $a \in A$ tal que $\sup A - \epsilon/2 < a$, y por la misma razón existe $b \in B$ tal que $\sup B - \epsilon/2 < b$, luego

$$\sup A + \sup B - \epsilon < a + b = z,$$

con $z \in A+B$. Usando nuevamente la propiedad de aproximación del supremo se tiene el resultado deseado. □

7.3. Raíces. Números Irracionales

Definición 7.27 (Irracionales)**.** *Un elemento de un campo ordenado F se dice irracional si éste no es racional, es decir, no puede ser representado como una razón m/n de un entero m y un natural n.*

En lo que viene probaremos que un campo ordenado completo los irracionales existen.

Lema 7.28. *Sean $n \in \mathbb{N}$ y $x, y \in F$ (con F un campo ordenado) tales que $x \geq 0$, $y > 0$.*

(*i*) *Si $x^n < y$, entonces existe $t > x$ tal que $t^n < y$.*

(*ii*) *Si $x^n > y$, entonces existe $0 < t < x$ tal que $t^n > y$.*

Prueba: Recordemos que si $n \in \mathbb{N}$ y $a, b \in F$, entonces

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}).$$

Ahora si $0 \leq b < a$, entonces

$$a^n = b^n + (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}) < b^n + (a-b)na^{n-1}.$$

(*i*) Supongamos que $x^n < y$. Sea h tal que

$$0 < h < \text{mín}\left\{1, \frac{y-x^n}{n(x+1)^{n-1}}\right\}.$$

Definamos $t := x+h$, entonces $t > x$ y

$$t^n < x^n + nh(x+h)^{n-1} \leq x^n + nh(x+1)^{n-1} < y.$$

Lo que termina la prueba de la primera parte del lema.

(*ii*) Supongamos que $x^n > y$. Tomemos h tal que

$$0 < h < \text{mín}\left\{x, \frac{x^n - y}{nx^{n-1}}\right\}.$$

En este caso consideremos $t := x - h$, entonces $0 < t < x$ y además

$$x^n < (x-h)^n + nhx^{n-1} < t^n + nx^{n-1}\left(\frac{x^n - y}{nx^{n-1}}\right) = t^n + x^n - y.$$

Por tanto $y < t^n$. □

Teorema 7.29. *Dado un elemento $a \geq 0$ en un campo ordenado completo F y un número natural $n \in \mathbb{R}$, siempre existe un único elemento $p \geq 0$ ($p \in F$) tal que $p^n = a$.*

Prueba: Si $a = 0$ el resultado es trivial, tome $p = 0$. Supongamos que $a > 0$ y definamos

$$M := \{t \geq 0 : t^n < a\}.$$

$M \neq \varnothing$ ya que $0 \in M$, además M está acotado superiormente. Veamos, por ejemplo, que $a+1$ es una cota superior de M. Para esto supongamos que $t \in M$ y $t > 1+a$, entonces $t^n > (1+a)^n > 1+a > a$, lo cual contradice el hecho de que $t^n < a$, pues $t \in M$. Por el axioma de completez existe el $\sup M =: p$. Claramente $p \geq 0$, veamos que $p^n = a$. En efecto, si $p^n < a$, entonces por lema anterior existe $t > p$ tal que $t^n < a$, o sea que $t \in M$ y $p < t$ lo cual es absurdo. Si $p^n > a$, entonces por lema anterior existe $0 < t < p$ tal que $t^n > a$. Ahora bien, si $u > t$ entonces $u^n > t^n > a$, es decir, $u \notin M$. Lo anterior quiere decir que si $u \in M$, entonces $u \leq t$. Por tanto t es una cota superior de M y $t < p$, lo cual es absurdo, así que $p^n = a$. □

Definición 7.30 (Raź $n-$ésima)**.** *El p dado por el Teorema anterior es llamado la raíz n-ésima de a y se denota como $\sqrt[n]{a}$ o $a^{\frac{1}{n}}$.*

Nota 7.31. (*i*) *Cuando $n = 2$, escribimos $\sqrt{a}$ en vez de $\sqrt[2]{a}$.*

(*ii*) *Si n es impar y $a < 0$, existe $p > 0$ tal que $p^n = -a$, luego $(-p)^n = -p^n = a$. Así cuando n es impar, para todo $a \in F$ existe un único $q \in F$ tal que $q^n = a$.*

Teorema 7.32. *Si x e y son elementos no negativos de un campo ordenado completo F y $n \in \mathbb{N}$, entonces*

$$\sqrt[n]{xy} = \sqrt[n]{x}\,\sqrt[n]{y}.$$

Prueba: Es dejada como ejercicio al lector.

Teorema 7.33. *Todo campo ordenado completo F contiene elementos irracionales. En particular, $\sqrt{2}$ es irracional.*

Prueba: La prueba es igual a la hecha en el Teorema 2.9. □

Teorema 7.34. *Si $n \in \mathbb{N}$, entonces $\sqrt{n} \in \mathbb{N}$ ó $\sqrt{n} \in \mathbb{I}$.*

Prueba: Supongamos que $\sqrt{n} \notin \mathbb{N}$ y $\sqrt{n} \in \mathbb{Q}$. Sean $q, p \in \mathbb{N}$ tales que $\sqrt{n} = p/q$, entonces $q\sqrt{n} = p \in \mathbb{N}$. Por lo tanto el conjunto $E = \{k \in \mathbb{N} : k\sqrt{n} \in \mathbb{Z}\} \neq \varnothing$. Sea $n_0 = \min E$, note que $n_0 \in \mathbb{N}$. De otro lado, existe $m_0 \in \mathbb{Z}$ tal que $m_0 < \sqrt{n} < m_0 + 1$, ya que $\sqrt{n} \notin \mathbb{N}$. Luego $0 < \sqrt{n} - m_0 < 1$. Multiplicando por n_0, obtenemos

$$0 < n_0\sqrt{n} - n_0 m_0 < n_0.$$

Definamos $x = n_0\sqrt{n} - n_0 m_0$, $x > 0$. Como $n_0 \in E$, entonces $x \in \mathbb{Z}^+ = \mathbb{N}$. Además $x\sqrt{n} = n_0 n - m_0(n_0\sqrt{n}) \in \mathbb{Z}$, luego $x \in E$ y $x < n_0$, lo cual es absurdo. □

7.4. Potencias con Exponente Real Arbitrario

Definición 7.35. *Dado un elemento $a \geq 0$ de un campo ordenado completo F y cualquier número racional $r = m/n > 0$ $(m, n \in \mathbb{N} \subseteq \mathbb{R})$, definimos $a^r = \sqrt[n]{a^m} = (a^m)^{\frac{1}{n}}$.*

Nota 7.36. *(i) Si $n = 1$, tenemos que $a^r = a^{m/1} = \sqrt[1]{a^m} = a^m$. Luego si $r \in \mathbb{N}$ $(\subseteq \mathbb{R})$, nuestra nueva definición coincide con la dada anteriormente.*

(ii) La definición anterior no depende de la representación particular de r en la forma m/n, por tanto no es ambigua. En efecto, supongamos que $r = m/n = p/q$, entonces $mq = np$, luego $a^{mq} = a^{np}$, entonces $(a^m)^q = (a^p)^n$. Por definición $\sqrt[n]{a^m}$ es exactamente el elemento cuya $n-$potencia es a^m, es decir,

$$a^m = (\sqrt[n]{a^m})^n,$$

Similarmente $(\sqrt[q]{a^p})^q = a^p$. Remplazando a^m y a^p en la ecuación $(a^m)^q = (a^p)^n$, tenemos, $(\sqrt[n]{a^m})^{nq} = (\sqrt[q]{a^p})^{qn}$, entonces $\sqrt[n]{a^m} = \sqrt[q]{a^p} = a^r$.

Teorema 7.37. *Sean $a, b \in F$ con $a > 0$, $b > 0$ y $r, s \in \mathbb{Q}$ con $r, s > 0$. Entonces*

(a) *Si $r = m/n$, $m \in \mathbb{Z}$ y $n \in \mathbb{N}$, entonces $(a^m)^{\frac{1}{n}} = (a^{\frac{1}{n}})^m$.*

(b) $a^r a^s = a^{r+s}$

(c) $(a^r)^s = a^{rs}$

(d) $(ab)^r = a^r b^r$

(e) *$a < b$ si y sólo si $a^r < b^r$*

(f) *$a^r < a^s$ si $0 < a < 1$ y $r > s$*

(g) *Si $a > 1$ y $r > s$, entonces $a^r > a^s$*

(h) $1^r = 1$

Prueba: Es dejada como ejercicio al lector.

A continuación vamos a definir a^x para cualquier real $x > 0$ y cualquier elemento $a > 1$ en un campo ordenado completo F. Tomemos

$$A_{ax} := \{a^r : 0 < r \leq x, \quad r \in \mathbb{Q}\}$$

Por la densidad de $\mathbb{Q}$ en $\mathbb{R}$, tales racionales existen, luego $A_{ar} \neq \varnothing$. Además A_{ar} es acotado superiormente en F. En efecto, sea $y > x$ con $y \in \mathbb{Q}$. Si $r \in \mathbb{Q}$ con $0 < r \leq x$, tenemos que

$$a^y = a^{r+(y-r)} = a^r a^{y-r} > a^r,$$

ya que $a > 1$ y $y - r > 0$, lo cual implica que $a^{y-r} > a^0 = 1$. Por tanto a^y es una cota superior para A_{ar}. Como F es completo tenemos que el $\sup A_{ar}$ existe, lo cual nos permite hacer la siguiente definición.

Definición 7.38. *Sean $a > 0$ en un campo completo F y $x \in \mathbb{R}$.*

(*i*) *Si $x > 0$ y $a > 1$, definimos*

$$a^x := \sup A_{ax}$$

(*ii*) *Si $x > 0$ y $0 < a < 1$, definimos*

$$a^x := \frac{1}{(1/a)^x},$$

que también se escribe como $(1/a)^{-x}$.

(*iii*) *Si $x > 0$, definimos $a^{-x} = 1/a^x$ (esto define potencias con exponente negativo)*

También definimos $0^x = 0$, para $x > 0$ y $a^0 = 1$, para $a \in F$, $a \neq 0$. Note que 0^0 sigue estando indefinido.

7.5. Sistema Ampliado de Números Reales

Por sistema ampliado de números reales, el cual denotaremos $\mathbb{R}^*$, entenderemos el conjunto de los números reales junto con dos símbolos $+\infty$ y $-\infty$ que satisfacen las siguintes propiedades:

(*i*) Si $x \in \mathbb{R}$, entonces $-\infty < x < +\infty$.

(*ii*) Si $x \in \mathbb{R}$, entonces

$$x + (+\infty) = +\infty, \quad x + (-\infty) = -\infty, \quad x - (+\infty) = -\infty, \quad x - (-\infty) = +\infty.$$

(*iii*) Si $x > 0$, entonces

$$x \cdot (+\infty) = +\infty, \quad x \cdot (-\infty) = -\infty.$$

(*iv*) Si $x < 0$, entonces

$$x \cdot (+\infty) = -\infty, \quad x \cdot (-\infty) = +\infty.$$

(*v*) $(+\infty)+(+\infty) = (+\infty)\cdot(+\infty) = (-\infty)\cdot(-\infty) = +\infty$ y además $(-\infty)+(-\infty) = (+\infty)\cdot(-\infty) = -\infty$.

Nota 7.39. (*i*) *NO permitimos los casos $(+\infty) + (-\infty)$, $0 \cdot (+\infty)$ y $0 \cdot (-\infty)$.*

(*ii*) *Los reales ampliados NO forman un campo.*

(*iii*) $\mathbb{R}^* = \mathbb{R} \cup \{+\infty, -\infty\} = [-\infty, +\infty]$ *y* $\mathbb{R} = (-\infty, +\infty)$.

(*iv*) *Los puntos de* $\mathbb{R}$ *se llaman "finitos" para diferenciarlos de los símbolos* $+\infty$ *y* $-\infty$.

Definición 7.40. *Sea* $E \subseteq \mathbb{R}$ *no vacío. Si* E *no es acotado superiormente definimos* $\sup E = +\infty$. *Si* E *no es acotado inferiormente definimos* $\inf E = -\infty$. *También definimos* $\inf \varnothing = +\infty$ *y* $\sup \varnothing = -\infty$. *Note que todo subconjunto de* $\mathbb{R}^*$ *tiene supremo e ínfimo en* $\mathbb{R}^*$.

7.6. Ejercicios

1. Sean $m, n \in \mathbb{Z}$, con $m \neq n$. Muestre que $|m - n| \geq 1$.

2. Sean $x, y \in \mathbb{R}^+$. Entonces:

 a) Si $m, p \in \mathbb{Z}$, $n, q \in \mathbb{N}$ y $m/n = p/q$, entonces $(x^m)^{1/n} = (x^p)^{1/q}$.

 b) Si $m, n \in \mathbb{N}$, entonces $(\sqrt[n]{x})^m = \sqrt[n]{x^m}$ y $\sqrt[n]{\sqrt[m]{x}} = \sqrt[nm]{x}$.

 c) Si $n \in \mathbb{N}$, entonces $\sqrt[n]{x}\,\sqrt[n]{y} = \sqrt[n]{xy}$.

3. Sean $x, y \in \mathbb{R}^+$ y $r, s \in \mathbb{Q}$. Probar que:

 a) $x^r x^s = x^{r+s}$.

 b) $(x^r)^s = x^{rs}$.

 c) $(xy)^r = x^r y^r$.

4. Sean $a, b \in \mathbb{R}$ con $a, b > 0$ y $x, y \in \mathbb{R}$. Probar que:

 a) $a^x a^y = a^{x+y}$.

 b) $(a^x)^y = a^{xy}$.

 c) $(ab)^x = a^x b^y$.

5. Sean $n \in \mathbb{N}$ y $0 \leq a < b$. Probar que $0 \leq a^n < b^n$ y $0 \leq \sqrt[n]{a} < \sqrt[n]{b}$.

6. Muestre que $\mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$ no son acotados inferiormente ni superiormente. Pruebe también que $\mathbb{N}$ no es acotado superiormente.

7. Calcule:
$$\text{máx}\left\{99^{50} + 100^{50},\, 101^{50}\right\}.$$

8. Sea $n \in \mathbb{N}$, muestre que $\left(1 + \frac{1}{2n}\right)^n - \left(1 - \frac{1}{2n}\right)^n \geq 1$.

9. *Propiedad de aproximación del ínfimo*: Sean E un subconjunto no vacío de $\mathbb{R}$ y $t \in \mathbb{R}$. Entonces $t = \inf E$ si y sólo si t es una cota inferior de E y para todo $\epsilon > 0$, existe $a \in E$ tal que $a < t + \epsilon$.

10. Sean E un subconjunto no vacío de $\mathbb{R}$. Entonces,

$$E \text{ es acotado si y sólo si existe } M > 0 \text{ tal que } |x| \leq M \text{ para todo } x \in E.$$

11. Pruebe que si x es cota superior de un conjunto no vacío $E \subsetneq \mathbb{R}$ y $x \in E$, entonces $x = \sup E$.

12. Sean X, Y subconjuntos no vacíos de $\mathbb{R}$ cuya unión es $\mathbb{R}$ y tales que cada elemento de X es menor que cada elemento de Y. Probar que existe $a \in \mathbb{R}$ tal que X es uno de los conjuntos

$$(-\infty, a) \text{ ó } (-\infty, a].$$

13. Probar que:

$$\sup\{x \in \mathbb{Q}^+ : x^2 < 2\} = \sqrt{2}.$$

14. Demostrar que cualquier conjunto inductivo no es acotado superiormente.

15. Sea E un subconjunto no vacío de $\mathbb{Z}$. Pruebe que :

 a) Si E es acotado superiormente, entonces $\sup E \in E$.

 b) Si E es acotado inferiormente, entonces $\text{ínf}\, E \in E$.

16. Probar que si A y B son subconjuntos no vacíos de $\mathbb{R}^+$ acotados superiormente, entonces $A \cdot B$ es acotado superiormente y

$$\sup(A \cdot B) = \sup A \cdot \sup B.$$

17. Sean A y B subconjuntos no vacíos de $\mathbb{R}$. Si A y B son acotados, entonces:

 a) $\sup(A \cup B) = \text{máx}\{\sup A, \sup B\}$,

 b) $\text{ínf}(A \cup B) = \text{mín}\{\text{ínf}\, A, \text{ínf}\, B\}$.

18. Si A es un subconjunto no vacío de $\mathbb{R}^+$ tal que $\text{ínf}\, A > 0$, entonces

$$\sup\left(\frac{1}{A}\right) = \frac{1}{\text{ínf}\, A}.$$

19. Si $a, b \in \mathbb{R}$ y $0 \leq a < b$, entonces existen $m, n \in \mathbb{N}$ tales que $a < m/10^n < b$.

20. *Algoritmo de la División*: Si $n, b \in \mathbb{Z}$ y $b > 0$, entonces existen enteros únicos q y r tales que:

 a) $n = bq + r$,

 b) $0 \leq r < b$.

21. Probar que si $x, y \in \mathbb{R}$, $n \in \mathbb{N}$ y $m \in \mathbb{Z}$, entonces:

 a) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.

 b) $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

 c) $\left\lfloor \dfrac{\lfloor x \rfloor + m}{n} \right\rfloor = \left\lfloor \dfrac{x + m}{n} \right\rfloor$.

 d) $\displaystyle\sum_{k=0}^{n-1} \left\lfloor x + \tfrac{k}{n} \right\rfloor = \lfloor nx \rfloor$.

22. Sea E un subconjunto no vacío de $\mathbb{R}^+$ acotado superiormente tal que

$$(\forall x, y \in E)\,(x < y \Longrightarrow x/y \in E).$$

Probar que si $\alpha := \sup E < 1$, entonces $\alpha \in E$.

23. Encontrar el supremo y el ínfimo de los siguientes conjuntos, sustentando en cada caso sus afirmaciones:

 a) $\{\frac{1}{3}, \frac{4}{9}, \frac{13}{27}, \frac{40}{81}, \ldots\}$

 b) $\{\frac{1}{2^p} + \frac{1}{3^q} + \frac{1}{5^r} : p, q, r \in \mathbb{N}\}$

 c) $\left\{\frac{m}{n} : m, n \in \mathbb{N},\ m < 2n\right\}$.

 d) $\left\{\frac{m}{m+n} : m, n \in \mathbb{N}\right\}$.

 e) $\{\sqrt{n} - \lfloor\sqrt{n}\rfloor : n \in \mathbb{N}\}$.

24. Demuestre:

 a) Si $a \in \mathbb{Q}$ y $b \in \mathbb{I}$, entonces $a + b \in \mathbb{I}$

 b) Si $a \in \mathbb{Q} \setminus \{0\}$ y $b \in \mathbb{I}$, entonces $ab \in \mathbb{I}$

 c) Si $a, b \in \mathbb{R}$ y $a < b$, entonces existe $i \in \mathbb{I}$ tal que $a < i < b$

 d) Si $a, b \in \mathbb{Q}^+$, entonces

 $$\sqrt{a} \in \mathbb{Q} \text{ y } \sqrt{b} \in \mathbb{Q} \text{ si y sólo si } \sqrt{a} + \sqrt{b} \in \mathbb{Q}$$

 e) Si $a, b, c, d \in \mathbb{Q},\ x \in \mathbb{I}$ y $cx + d \neq 0$, entonces

 $$\frac{ax + b}{cx + d} \in \mathbb{I} \text{ si y sólo si } ad \neq bc.$$

25. *a*) Probar que $\sqrt{n-1} + \sqrt{n+1}$ es irracional para todo $n \in \mathbb{N}$.

 b) Probar que $\sqrt{n+3} + \sqrt{n}$ es racional para algún $n \in \mathbb{N}$ si y sólo si $n = 1$.

 c) Probar que $\sqrt{n+7} + \sqrt{n}$ es racional para algún $n \in \mathbb{N}$ si y sólo si $n = 9$.

26. Sean $\lambda \in \mathbb{I}$ y $E := \{n\lambda + m : m \in \mathbb{Z},\ n \in \mathbb{N}\}$. Probar que dados $x \in \mathbb{R}$ y $\epsilon > 0$, entonces existe $t \in E$ tal que $|x - t| < \epsilon$. *Sugerencia* : Pruebe que dado $N \in \mathbb{N}$ existe $a \in E$ tal que $|a| < \frac{1}{N}$.

27. Sea x un número real. Muestre que por lo menos uno de los números $\sqrt{2} - x$ o $\sqrt{2} + x$ es irracional.

28. Muestre que $\sqrt{2} + \sqrt{3}$ y $2 + \sqrt{3}$ son irracionales.

29. Hallar el supremo y el ínfimo (si existen) de los siguientes conjuntos:

 a) $A = \left\{-\frac{1}{n} + n^2[1 + (-1)^n] : n \in \mathbb{N}\right\}$.

 b) $B = \left\{\frac{2+n}{n} : n \in \mathbb{N}\right\}$.

 c) $C = \left\{(-1)^n - \frac{1}{n} : n \in \mathbb{N}\right\}$.

 d) $D = \{[1 - (-1)^n]^n : n \in \mathbb{N}\}$.

 e) $E = \left\{[\frac{3}{2} + (-1)^n]^n : n \in \mathbb{N}\right\}$.

30. Sean $x, y \in F$, donde F es un campo arquimediano, con $x < y$ y $y - x > 1$. Muestre que existe $m \in \mathbb{Z}$ tal que $x \leq m \leq y$.

31. Sean $x, y \in F$, donde F es un campo arquimediano, con $x < y$ y $y - x < 1$. Muestre que $\lfloor y \rfloor - \lfloor x \rfloor = 0$ ó 1.

32. *a*) Muestre que para todo elemento x en un campo arquimediano F, siempre existe un único entero $m \in F$, tal que

$$m - 1 < x \leq m.$$

A tal m lo denotaremos por $\lceil x \rceil$.

b) Muestre que $\lceil x \rceil = -\lfloor -x \rfloor$

Capítulo 8

Cardinalidad.

De manera intuitiva el cardinal nos indica el número o cantidad de elementos que tiene un conjunto, este concepto para conjuntos finitos es bastante claro y de una u otra forma caracteriza los conjuntos. Ya para conjuntos con un número infinito de elementos la situación es mucho más complicada, por ejemplo es díficil creer que los naturales y los racionales tengan la misma cantidad de elementos (algo que probaremos más adelante) y que a pesar de la densidad de los racionales y reales, estos no tengan la misma cardinalidad. El objetivo de este capítulo es precisar los conceptos de finito, infinito, numerable, contable y no contable. Básicamente estudiaremos las ideas de Georg Cantor (1845-1918), quien en una serie de artículos amplió la teoría de cardinales a conjuntos infinitos usando conceptos simples de funciones como lo son la inyectividad y sobreyectividad. Cantor esencialmente organizó todas la ideas desordenadas que existian hasta ese momento sobre cardinalidad y logró obtener algunos resultados que eran insospechados hasta ese momento como lo veremos a continuación.

8.1. Conjuntos Equipotentes; Conjuntos Finitos

Para determinar si dos conjuntos tienen el mismo número de elementos, veremos si es posible colocarlos en una correspondencia uno a uno, tal como lo hacemos en nuestra vida diaria. Esta idea es conveniente describirla en términos de correspondecia inyectiva (o mejor una biyección) de un conjunto en otro, como sigue.

Definición 8.1 (Conjuntos equipotentes)**.** *Dos conjuntos A y B se dicen equipotentes (o que tienen la misma cardinalidad), denotado $A \sim B$, si existe una función biyectiva de A en B.*

Es claro que si dos conjuntos son equipotentes, habrá muchas funciones biyectivas entre ellos. (A menos que cada conjunto solo tenga uno o cero elementos).

Lema 8.2. *Sean A, B y C conjuntos*

(*i*) $A \sim A$

(*ii*) $A \sim B$, *entonces* $B \sim A$

(*iii*) $A \sim B$ *y* $B \sim C$, *entonces* $A \sim C$

Prueba:

(*i*) Sea $I : A \to A$ definida como $I(x) = x$, para todo $x \in A$ (la función identidad) claramente I es biyectiva.

(*ii*) Supongamos que $A \sim B$, entonces existe una función $f : A \to B$ tal que f es biyectiva. Por la biyectividad de f, existe $f^{-1} : B \to A$. Recordemos que $f^{-1}(y) = x$ si y sólo si $f(x) = y$. Se prueba fácilmente que f^{-1} es biyectiva.

(*iii*) Supongamos que $A \sim B$ y $B \sim C$. Entonces existen $f : A \to B$ y $g : B \to C$, funciones biyectivas. Definamos $h = g \circ f$. Por la biyectividad de f y g, se prueba que h es biyectiva. □

Nota 8.3. *Lo que indica el lema anterior es que* $\sim$ *es una relación de equivalencia sobre cualquier familia de conjuntos.*

Ejemplo 8.4. $\mathbb{N} = \{1, 2, 3, ...\}$ *y* $S = \{1, 4, 9, 16, ...\}$ *tienen la misma cardinalidad. En efecto, defina* $h : \mathbb{N} \to S$ *por* $h(n) = n^2$, *es fácil ver que* h *es biyectiva.*

Ejemplo 8.5. $\mathbb{N} \sim \mathbb{Z}$. *En efecto, definamos* $f : \mathbb{Z} \to \mathbb{N}$, *por*

$$f(n) = \begin{cases} -2n, & si\ n < 0 \\ 2n + 1, & si\ n \geq 0 \end{cases}$$

se verifica fácilmente que f *es biyectiva.*

Ejemplo 8.6. *Sean* $a, b, c, d \in \mathbb{R}$, *entonces* $[a, b] \sim [c, d]$, *donde* $a < b$ *y* $c < d$. *En efecto, definamos* $g : [a, b] \to [c, d]$ *por*

$$g(x) = \left(\frac{d-c}{b-a}\right)(x - a) + c.$$

Veamos que g *es sobre. Sea* $y \in [c, d]$ *y considere* $x = \dfrac{(y-c)(b-a)}{(d-c)} + a$. *Note que* $x \in [a, b]$ *y*

$$g(x) = \frac{d-c}{b-a}\left(\frac{(y-c)(b-a)}{(d-c)} + a - a\right) + c = y.$$

Por tanto g *es sobre. El resto de la prueba es dejada al lector.*

Proposición 8.7. *Si* $a, b \in \mathbb{R}$ *con* $a < b$. *Dos cualesquiera de los siguientes conjuntos tienen la misma cardinalidad:*

$$(0, 1), [a, b], [a, b), (a, b], (a, b), [a, +\infty), (a, +\infty), (-\infty, b], (-\infty, b) \quad y \quad (-\infty, +\infty).$$

Prueba:

(*i*) Veamos que $(0,1) \sim (a,b)$. Definamos $f : (0,1) \to (a,b)$ por $f(x) = a + x(b-a)$. Es fácil ver que f es biyectiva.

(*ii*) Veamos que $(0,1) \sim (0,+\infty)$. En efecto, definase $g : (0,1) \to (0,+\infty)$ por $g(x) = \dfrac{1}{x} - 1$. Es fácil ver la biyectividad de g, luego por la transitividad $(a,b) \sim (0,+\infty)$. Además $(0,+\infty) \sim (a,+\infty)$. Para eso tome $h : (0,+\infty) \to (a,+\infty)$ como $h(x) = x + a$, facilmente se prueba que h es biyectiva. luego $(a,b) \sim (a,+\infty)$.

(*iii*) Veamos que $(0,1) \sim (-\infty,+\infty)$. Definamos

$$h(x) = \begin{cases} 2 - \dfrac{1}{x}, & x \in (0, \frac{1}{2}) \\ \dfrac{1}{1-x} - 2, & x \in [\frac{1}{2}, 1). \end{cases}$$

para $x \in (0,1)$. La prueba de que h es inyectiva es dejada al lector, probaremos que h es sobre. Para eso considere $y \in (-\infty,+\infty)$, entonces $y \in (-\infty,0)$ ó $y \in [0,+\infty)$. Si $y \in (-\infty,0)$, existe $x = \dfrac{1}{2-y} \in (0,\frac{1}{2})$ tal que $h(x) = y$. Si $y \geq 0$, existe $x = 1 - \dfrac{1}{y+2} \in [\frac{1}{2},1)$ tal que $h(x) = y$. Lo que muestra que h es biyectiva.

(*iv*) $(0,1) \sim (-\infty,0)$. En efecto considere $g(x) = 1 - \dfrac{1}{x}$, $x \in (0,1)$.

(*v*) $(0,1] \sim (-\infty,0]$. Sea $g(x) = 1 - \dfrac{1}{x}$, $x \in (0,1]$.

(*vi*) $(0,1] \sim [0,+\infty)$. En efecto definamos $g(x) = -1 + \dfrac{1}{x}$, $x \in (0,1]$.

(*vii*) Veamos que $[0,1] \sim (0,1)$. Sea $A = [0,1] \backslash \{0, 1, 1/2, 1/3, ...\} = (0,1) \backslash \{1/2, 1/3, 1/4, ...\}$ Note que

$$[0,1] = \{0, 1, 1/2, 1/3, ...\} \cup A \quad \text{y} \quad (0,1) = \{1/2, 1/3, 1/4, ...\} \cup A$$

Consideremos la función $f : [0,1] \to (0,1)$ definida como

$$f(x) = \begin{cases} \dfrac{1}{2}, & x = 0 \\ \dfrac{1}{n+2}, & \text{si } x = 1/n, \text{ para algún } n \in \mathbb{N} \\ x, & \text{en otro caso.} \end{cases}$$

f es inyectiva y sobre.

(*viii*) $(0,1] \sim (0,1)$. En efecto definamos para todo $x \in (0,1]$

$$f(x) = \begin{cases} \dfrac{1}{n+1}, & \text{si } x = 1/n, \text{ para algún } n \in \mathbb{N} \\ x, & \text{en otro caso.} \end{cases}$$

f es también inyectiva y sobre.

(ix) $[0,1) \sim (0,1]$. En efecto, sea $f : [0,1) \to (0,1]$ dada por $f(x) = 1-x$, f es claramente biyectiva.

Definición 8.8. *Sea $n \in \mathbb{N}$. Definimos $J_n = \{i \in \mathbb{N} : i \leq n\}$, es decir, $J_n = \{1, 2, ..., n\}$.*

Definición 8.9. *Sea A un conjunto. Decimos que:*

(i) *A es finito si $A = \varnothing$ ó existe $n \in \mathbb{N}$ tal que $A \sim J_n$.*

(ii) *A es infinito si A no es finito.*

(iii) *A es numerable si $A \sim \mathbb{N}$.*

(iv) *A es contable si A es finito ó A es numerable .*

(v) *A es no-contable si A no es contable.*

Teorema 8.10. *Sea $A \subset J_n$. Si $A \sim J_n$, entonces A=J_n.*

Prueba: Usaremos inducción sobre n. Supongamos que $n = 1$ y sea $A \subset J_1$, tal que $A \sim J_1$. Como $A \subset J_1$, entonces $A = \varnothing$ o $A = J_1$, pero $A \neq \varnothing$ y así $A = J_1$. Supongamos que el resultado se tiene para algún $n \in \mathbb{N}$. Sean $A \subset J_{n+1}$ y $f : J_{n+1} \to A$ biyectiva, mostraremos que $A = J_{n+1}$. Para esto defina $a := f(n+1)$ *y* $f' := f|_{J_n} : J_n \to A - \{a\}$. Note que f' es biyectiva. Considere los siguentes casos: $(i) A - \{a\} \subset J_n$: Aquí , por la hipótesis inductiva, $A - \{a\} = J_n$, luego $a = n+1$ y $A = A - \{a\} \cup \{a\} = J_{n+1}$ $(ii) A - \{a\} \nsubseteq J_n$. Aquí, existe b $\in A - \{a\}$ y b no pertenece a J_n, entonces $b = n+1$ y así $n+1 \in A - \{a\}$. Sea $p \in J_{n+1}$ tal que $f(p) = n+1$. Definamos $g : J_{n+1} \to A$ por:

$$g(x) = \begin{cases} f(x) & \text{si } x \text{ no pertenece a } \{p, n+1\} \\ a & \text{si } x = p \\ n+1 & \text{si } x = n+1 \end{cases}$$

Se puede verificar que g es biyectiva. Luego, $g' = g|_{J_n} : J_n \to A - \{n+1\}$ es biyectiva. Como $A - \{n+1\} \subset J_n$, por la hipotesis inductiva $A - \{n+1\} = J_n$ y así $A = J_{n+1}$ □

La prueba del siguiente corolario es dejada como ejercicio al lector.

Corolario 8.11. *Sean $m, n \in \mathbb{N}$. Entonces $J_n \sim J_m$ si y sólo si $m = n$.*

Definición 8.12 (Cardinalidad)**.** *Sea A un conjunto finito. Definimos la cardinalidad de A, denotado $|A|$, como sigue: Si $A = \varnothing$, ponemos $|A| = 0$. Si $A \neq \varnothing$, definimos $|A| = n$, donde $A \sim J_n$.*

Corolario 8.13. *Sean A y B conjuntos finitos no vacíos. Entonces $A \sim B$ si y sólo si $|A| = |B|$.*

Prueba: " $\Rightarrow$ " Como $A, B \neq \varnothing$ y $A \sim B$, existen $m, n \in \mathbb{N}$ tales que $A \sim J_n$ y $B \sim J_m$. Por tanto $J_n \sim J_m$ y el lema anterior implica que $n = m$, luego $|A| = n = m = |B|$.
" $\Leftarrow$ " Supongamos que $|A| = |B| = n$, entonces $A \sim J_n$ y $B \sim J_n$, luego por transitividad $A \sim B$.
□

Ejemplo 8.14. *Sea* $B = \{1, 4, 9, 16\}$. *Probar que* $|B| = 4$. *Sea* $h : B \to J_4$, *definida por* $h(x) = \sqrt{x}$. *Fácilmente se verifica que* h *es biyectiva, luego* $|B| = 4$.

A continuación presentamos dos resultados que son bastante usados en estadística.

Teorema 8.15. *Sean* A *y* B *conjuntos finitos. Si* $A \cap B = \varnothing$, *entonces*

$$|A \cup B| = |A| + |B|.$$

Prueba: Si A o B es vacío el resultado es inmediato. Supongamos que $|A| = n$ y $|B| = m$, entonces existen biyecciones $f : A \to J_n$ y $g : B \to J_m$. Considere $h : A \cup B \to J_{n+m}$ dada por

$$h(x) = \begin{cases} f(x), & \text{si } x \in A \\ n + g(x), & \text{si } x \in B. \end{cases}$$

Veamos que h es inyectiva. Tome $x_1, x_2 \in A \cup B$ tales que $h(x_1) = h(x_2)$. Pueden ocurrir cuatro casos: $x_1, x_2 \in A$, $x_1, x_2 \in B$, $x_1 \in A; x_2 \in B$ y $x_1 \in B; x_2 \in A$. Sólo analizaremos dos de estos casos pues los otros son análogos. Caso 1: Si $x_1, x_2 \in A$, entonces $f(x_1) = h(x_1) = h(x_2) = f(x_2)$ y como f es inyectiva en A se tiene que $x_1 = x_2$. Caso 2: $x_1 \in A; x_2 \in B$. Veremos que este caso en realidad no se presenta. Tenemos que $f(x_1) = h(x_1) = h(x_2) = n + g(x_2)$. Así que $f(x_1) = n + g(x_2) > n$, lo cual es absurdo, pues $f(x_1) \in J_n$. Por tanto h es inyectiva.

Mostraremos ahora que h es sobre, para eso tome $y \in J_{n+m}$. Entonces $1 \leq y \leq n$ ó $n < y \leq m+n$. En el primer caso por la sobreyectividad de f se garantiza la existencia de $x \in A \subset A \cup B$ tal que $h(x) = f(x) = y$. Si $n < y \leq m + n$, entonces $0 < y - n \leq m$ y por las propiedades de g existe $x \in B \subset A \cup B$ tal que $g(x) = y - n$. Lo que es equivalente a $h(x) = n + g(x) = y$, pues $x \in B$. Lo que muestra que h es sobreyectiva y esto termina la prueba. □

Aplicando inducción es fácil probar el siguiente resultado.

Corolario 8.16. *Sean* $X_1, X_2, X_3, ..., X_k$ *conjuntos finitos, disjuntos dos a dos tales que* $|X_i| = m_i$, *para* $i = 1, 2, 3, ..., k$. *Entonces* $\bigcup_{i=1}^{k} X_i$ *es finito y* $|\bigcup_{i=1}^{k} X_i| = \sum_{i=1}^{k} m_i$.

Corolario 8.17. *Sean* A *y* B *conjuntos finitos. Entonces*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Prueba: *Defina* $F = A - (A \cap B)$ *y* $G = B - (A \cap B)$. *Claramente las parejas* F *y* G; F *y* $A \cap B$; G *y* $A \cap B$ *son disyuntas. Además*

$$A = F \cup (A \cap B) \quad y \quad B = G \cup (A \cap B).$$

Por el Teorema 8.15 se tiene que

$$|A| = |F| + |A \cap B| \quad y \quad |B| = |G| + |A \cap B|. \tag{8.1}$$

Ahora, como $A \cup B = (F \cup G) \cup (A \cap B)$ y la pareja $F \cup G$; $A \cap B$ es disyunta, usando nuevamente el Teorema 8.15 y (8.1) se obtiene

$$\begin{aligned} |A \cup B| &= |F \cup G| + |A \cap B| = |F| + |G| + |A \cap B| \\ &= |B| - |A \cap B| + |A| - |A \cap B| + |A \cap B| = |A| + |B| - |A \cap B|. \end{aligned}$$

Lo que termina la prueba. □

Lema 8.18. *Sean $n \in \mathbb{N}$ y $S \subseteq J_n$ no vacío. Entonces existen una biyección $h : J_n \to J_n$ y $k \leq n$ natural tales que $h_*(S) = J_k$.*

Prueba: Definamos

$$G = \{n \in \mathbb{N} : \text{La conclusión de lema es valida para } \ S \subseteq J_n, S \neq \varnothing\}.$$

Veamos que G es inductivo. $1 \in G$ ya que si $S \subseteq J_1$, $S \neq \varnothing$, entonces $S = \{1\}$. Así que existe $h : J_1 \to J_1$ con $h(1) = 1$, tal que $h_*(S) = \{1\} = J_1$.
Supongamos que $n \in G$, mostraremos que $n+1 \in G$. Sea $S \subseteq J_{n+1}$, con $S \neq \varnothing$. Pueden ocurrir dos casos:
Caso 1: $n+1 \notin S$, entonces $S \subseteq J_n$. Por hipótesis inductiva existen $h : J_n \to J_n$ biyectiva y k natural con $k \leq n$, tales que $h_*(S) = J_k$. Consideremos $\psi : J_{n+1} \to J_{n+1}$ dada por

$$\psi(m) = \begin{cases} h(m), & \text{si } m \in J_n \\ n+1, & \text{si } m = n+1. \end{cases}$$

ψ es biyectiva y $\psi_*(S) = h_*(S) = J_k$ donde $k \leq n < n+1$.
Caso 2: $n+1 \in S$. En este caso definimos $B = S - \{n+1\}$. Si $B = \varnothing$, entonces $S = \{n+1\}$. Tomando $\psi : J_{n+1} \to J_{n+1}$, como

$$\psi(m) = \begin{cases} m, & \text{si } m \in J_n - \{1\} \\ n+1, & \text{si } m = 1 \\ 1, & \text{si } m = n+1. \end{cases}$$

tendriamos que ψ es biyectiva y $\psi_*(S) = J_1$, con $1 \leq n+1$. Supongamos que $B \neq \varnothing$, por tanto $B \subseteq J_n$. Usando la hipótesis inductiva, existe $h : J_n \to J_n$ biyectiva y k natural con $k \leq n$, tales que $h_*(B) = J_k$. Definamos $\psi : J_{n+1} \to J_{n+1}$ como

$$\psi(m) = \begin{cases} h(m), & \text{si } m \in J_n - \{h^{-1}(k+1)\} \\ n+1, & \text{si } m = h^{-1}(k+1) \\ k+1, & \text{si } m = n+1. \end{cases}$$

ψ es biyectiva, además $\psi_*(S) = \psi_*(B \cup \{n+1\}) = \psi_*(B) \cup \psi_*(\{n+1\}) = J_k \cup \{k+1\} = J_{k+1}$. Como $k+1 \leq n+1$, se tiene que $n+1 \in G$. Lo que termina la prueba del lema. □

Teorema 8.19. *Sea A un conjunto finito.*

(*i*) *Si* $X \subseteq A$, *entonces* X *es finito.*

(*ii*) *Si* $X \subseteq A$, *entonces* $|A| = |X| + |A - X|$.

(*iii*) *Si* $X \subsetneq A$, *entonces* $|X| < |A|$.

(*iv*) *Si* $X \subsetneq A$, *entonces* $X \nsim A$.

Prueba:

(*i*) Si $X = \varnothing$ el resultado es claro. Supongamos que $X \neq \varnothing$. Como A es finito, existe $h : A \to J_n$ biyectiva. Como $h_*(X) \subseteq J_n$, por el lema anterior existe $g : J_n \to J_n$ biyectiva y $k \leq n$ tales que $g_*(h_*(X)) = J_k$. Por tanto $h_*(X) \sim J_k$ y como $X \sim h_*(X)$, obtenemos el resultado deseado.

(*ii*) Note que $A = X \cup (A - X)$ y que $X \cap (A - X) = \varnothing$. Por tanto del Teorema 8.15 se obtiene el resultado deseado.

(*iii*) Como $X \neq A$, entonces $|A - X| > 0$, por tanto $|A| = |X| + |A - X| > |X|$.

(*iv*) Suponga que $X \sim A$, entonces por por Corolario 8.13 se tiene que $|X| = |A|$, pero por (*iii*) ésto es absurdo. □

Teorema 8.20. *Sean* X, Y *conjuntos finitos tales que* $|X| = m$ *y* $|Y| = n$. *Entonces* $X \times Y$ *es finito y* $|X \times Y| = mn$

Prueba: Como $Y \sim J_n$ podemos escribir $Y = \{y_1, y_2, y_3, ..., y_n\}$ con $y_j \neq y_i$ para todo $i \neq j$. Para cada $i \in J_n$, defina $X_i := X \times \{y_i\}$. Claramente

$$X \times Y = \bigcup_{i=1}^{n} X_i.$$

Además $|X_i| = |X| = m$ y $X_i \cap X_j = \varnothing$ si $i \neq j$. Luego por el Corolario 8.16 se tiene que $X \times Y$ es finito y $|X \times Y| = |\bigcup_{i=1}^{n} X_i| = \sum_{i=1}^{n} m = mn$. □

8.2. Conjuntos Infinitos y Contables

En esta sección discutiremos varios resultados importantes sobre conjuntos infinitos y contables, veremos que no todos los conjuntos infinitos son equipotentes y determinaremos la cardinalidad de los racionales. En la sección anterior definimos los conjuntos infinitos como aquellos que no se pueden poner en correspondencia inyectiva con un segmento inicial J_k, con k un entero positivo, y los conjuntos contables son aquellos que son finitos o son numerables. El siguiente resultado nos da otra forma de determinar sin un conjunto es infinito.

Corolario 8.21. *Sea A un conjunto. Entonces A es infinito si y sólo si A contiene un subconjunto infinito.*

Prueba: " $\Rightarrow$ " Suponga que A es infinito. Como $A \subseteq A$ podemos tomar A como el subconjunto infinito de A.
" $\Leftarrow$ " Sea $B \subseteq A$ con B infinito. Si A fuera finito, por teorema anterior parte (i) tendríamos que B seria finito, lo cual es absurdo. □

Es claro que para usar el corolario anterior necesitamos conocer algún conjunto infinito, el siguiente teorema nos dice que $\mathbb{N}$ es uno de tales conjuntos.

Teorema 8.22. $\mathbb{N}$ *es infinito.*

Prueba: Supongamos que $\mathbb{N}$ es finito. Como $\mathbb{N} \neq \varnothing$, existe $n \in \mathbb{N}$ tal que $\mathbb{N} \sim J_n$. Pero $n+1 \in \mathbb{N}$ y $n+1 \notin J_n$, así que $\mathbb{N} \subsetneq J_n$. Usando el Teorema 8.19 se tiene que $\mathbb{N} \nsim J_n$, lo cual es absurdo. □

Corolario 8.23. *Todo conjunto numerable es infinito.*

Prueba: Sea A un conjunto numerable. Razonando por el absurdo, supongamos que A es finito. Como $A \neq \varnothing$, entonces $A \sim J_n$, para algún $n \in \mathbb{N}$. Como $A \sim \mathbb{N}$ y $A \sim J_n$, se tiene que $\mathbb{N} \sim J_n$, lo cual contradice el teorema anterior. □

Nota 8.24. *Se probó anteriormente que $\mathbb{Z} \sim \mathbb{N}$, por tanto tenemos que $\mathbb{Z}$ es numerable.*

Teorema 8.25. *Todo subconjunto de $\mathbb{N}$ es contable.*

Prueba: Sea $A \subseteq \mathbb{N}$. Si A es finito listo, A es contable. Supongamos que A es infinito. Construiremos inductivamente una función biyectiva $\phi : \mathbb{N} \to A$ de la siguiente forma. Definamos $\phi(1) = \min A$, como A es infinito, $A \neq \varnothing$, luego por el P.B.O. $\min A$ existe, así que $\phi(1)$ está bien definido. Supongamos que ya hemos definido $\phi(1), \phi(2), ..., \phi(n)$ con $n \in \mathbb{N}$. Consideremos $\phi(n+1) = \min(A - \{\phi(1), \phi(2), ..., \phi(n)\})$. Como A es infinito, entonces $A - \{\phi(1), \phi(2), ..., \phi(n)\} \neq \varnothing$, luego por el P.B.O. $\phi(n+1)$ está bien definida. Veamos que ϕ es biyectiva: Claramente $\phi(1) < \phi(2)$. Sea $n \in \mathbb{N}$ con $n > 1$. Como

$$\phi(n+1) \in A - \{\phi(1), \phi(2), ..., \phi(n)\} \subseteq A - \{\phi(1), \phi(2), ..., \phi(n-1)\}.$$

Así que $\phi(n) < \phi(n+1)$. Por tanto ϕ es inyectiva. Sea $m \in A$ y $B = \{k \in A : k \leq m\}$. Como $B \subseteq J_m$, B es finito. Sea n el número de elementos de B. Como $m \in B$ se tiene que $n \in \mathbb{N}$, luego por la forma como se construyo ϕ se tiene que $\phi(n) = m$. Así que ϕ es sobre. □

Corolario 8.26. *Todo subconjunto de un conjunto contable es contable.*

Prueba: Sea A un conjunto contable y $B \subseteq A$ se tienen dos casos.
Caso 1: A es finito, por teorema anterior B es finito, por tanto B es contable.

Caso 2: A es infinito. Como A es contable, entonces A es numerable, es decir, existe $\varphi : A \to \mathbb{N}$ biyectiva. Como $\varphi_*(A) = \mathbb{N}$ y $\varphi_*(B) \subseteq \varphi_*(A) = \mathbb{N}$, se tiene que $\varphi_*(B)$ es contable. Como $B \sim \varphi_*(B)$ y $\varphi_*(B) \sim \mathbb{N}$ o $\varphi_*(B) \sim J_n$, obtenemos que B es contable. □

Teorema 8.27. *Sea A un conjunto no vacío. Las siguientes afirmaciones son equivalentes*

(*i*) *A es contable.*

(*ii*) *Existe una función $f : A \to \mathbb{N}$ inyectiva.*

(*iii*) *Existe una función $f : \mathbb{N} \to A$ sobreyectiva.*

Prueba: $(i) \Rightarrow (iii)$ Si A es finito, existe $n \in \mathbb{N}$ y $f : J_n \to A$ biyectiva. Definamos $g : \mathbb{N} \to J_n$ como

$$g(k) = \begin{cases} k & , \ k \leq n, \\ 1 & , \ k > n. \end{cases}$$

g es sobreyectiva. Por tanto $h := f \circ g : \mathbb{N} \to A$ es sobreyectiva. Si A es infinito el resultado es claro.
$(iii) \Rightarrow (ii)$ Sea $g : \mathbb{N} \to A$ sobreyectiva. Definamos $f : A \to \mathbb{N}$ por $f(a) = \text{mín}\, g^*(\{a\})$. Como $g^*(\{a\}) \neq \varnothing$ y $g^*(\{a\}) \subseteq \mathbb{N}$, entonces por el P.B.O. $f(a)$ está bien definido. Veamos que f es inyectiva. Sean $a_1, a_2 \in A$ con $a_1 \neq a_2$. Entonces

$$g^*(\{a_1\}) \cap g^*(\{a_2\}) \neq \varnothing.$$

Así que $f(a_1) \neq f(a_2)$.
$(ii) \Rightarrow (i)$ Supongamos que existe $f : A \to \mathbb{N}$ inyectiva. Como $f_*(A) \subseteq \mathbb{N}$, entonces $f_*(A)$ es contable. Puesto que $A \sim f_*(A)$, tenemos que A es contable. □

Teorema 8.28. *Si A y B son contables, entonces $A \times B$ es contable.*

Prueba: Veamos primero que existe una función inyectiva $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. En efecto definamos $f(m, n) = n + 2^{m+n}$, para todo $(m, n) \in \mathbb{N} \times \mathbb{N}$. Supongamos que

$$f(m, n) = f(j, k) \quad \text{y} \quad n \geq k.$$

Entonces $n + 2^{m+n} = k + 2^{j+k}$ y $0 \leq n - k = 2^{j+k} - 2^{m+n} < n$. Como $n < 2^n < 2^{m+n}$, entonces $2^{m+n} \leq 2^{j+k} < n + 2^{m+n} < 2^{m+n} + 2^{m+n} = 2^{m+n+1}$. Por lo tanto $m + n \leq j + k < m + n + 1$, es decir $j + k = m + n$. Luego $n - k = 2^{j+k} - 2^{m+n} = 0$, así que $n = k$ y consecuentemente $m = j$. En el caso $n < k$, hacemos el mismo racionamiento cambiando n por k y llegamos a que este caso no se puede presentar.

Ahora, supongamos que A y B son contables; entonces existen funciones inyectivas $\varphi : A \to \mathbb{N}$ y $\psi : B \to \mathbb{N}$. Definamos $h : A \times B \to \mathbb{N} \times \mathbb{N}$, como $h(a, b) = (\varphi(a), \psi(b))$. Claramente h es inyectiva. Por lo tanto la función $f \circ h : A \times B \to \mathbb{N}$ es inyectiva, lo que prueba que $A \times B$ es contable. □

Es interesante observar que en la prueba del teorema anterior se mostró que existe una función $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ inyectiva. Usando el Teorema 8.27 se concluye que $\mathbb{N} \times \mathbb{N}$ es contable. Como $\mathbb{N} \times \{1\} \subset \mathbb{N} \times \mathbb{N}$ y $\mathbb{N} \times \{1\} \sim \mathbb{N}$, se concluye que $\mathbb{N} \times \mathbb{N}$ es numerable.

Corolario 8.29. $\mathbb{Q}$ *es contable.*

Prueba: Como $\mathbb{Z}$ y $\mathbb{N}$ son contables, entonces por el teorema anterior $\mathbb{Z}\times\mathbb{N}$ es contable. Por teorema anterior existe $\varphi : \mathbb{N} \to \mathbb{Z} \times \mathbb{N}$ sobreyectiva. De otro lado $\psi : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ dada por $\psi(m, n) = m/n$ es sobreyectiva. Por lo tanto, $\psi \circ \varphi : \mathbb{N} \to \mathbb{Q}$ es sobreyectiva, así que $\mathbb{Q}$ es contable. □

Nota 8.30. (*i*) *Como* $\mathbb{N} \subset \mathbb{Q}$, *entonces* $\mathbb{Q}$ *es infinito, por tanto* $\mathbb{Q}$ *es numerable.*
(*ii*) *Por inducción se puede probar que si* $A_1, ..., A_n$ *son contables, entonces*

$$A_1 \times A_2 \times \cdots \times A_n$$

es contable.

Teorema 8.31. *Sean* I *un conjunto no vacío y* $\{A_i\}_{i\in I}$ *una familia de conjuntos contables, (i.e.,* A_i *es contable para todo* $i \in I$*). Entonces*

(*i*) $\bigcap_{i\in I} A_i$ *es contable.*

(*ii*) *Si* I *es contable, entonces* $A = \bigcup_{i\in I} A_i$ *es contable.*

Prueba:

(*i*) Sea $k_0 \in I$, entonces $\bigcap_{k\in I} A_k \subseteq A_{k_0}$, como A_{k_0} es contable, entonces por teorema anterior $\bigcap_{k\in I} A_k$ es contable.

(*ii*) Supongamos que $A_i \neq \varnothing$, para todo $i \in I$. Por teorema anterior existen funciones sobreyectivas $g : \mathbb{N} \to I$ y $f_i : \mathbb{N} \to A_i$ para cada $i \in I$. Definamos $h : \mathbb{N} \times \mathbb{N} \to A$ por $h(m, n) = f_{g(m)}(n)$, mostraremos que h es sobreyectiva. En efecto, sea $a \in A$, entonces existe $i \in I$ tal que $a \in A_i$, por lo tanto existen $m, n \in \mathbb{N}$ tales que $g(m) = i$ y $f_i(n) = a$. Luego $h(m, n) = f_{g(m)}(n) = f_i(n) = a$. Ahora, como $\mathbb{N}\times\mathbb{N}$ es contable, existe $\varphi : \mathbb{N} \to \mathbb{N}\times\mathbb{N}$ sobre, por tanto $h\circ\varphi : \mathbb{N} \to A$ es sobre. □

8.3. Conjuntos no Contables

En esta sección mostraremos la existencia de conjuntos no contables, para eso comencemos con un ejemplo.

Ejemplo 8.32. *Sea* $A = \{1, 2\}$. *Entonces* $\mathscr{P}(A) = \{\varnothing, \{1\}, \{2\}, A\}$. *Por tanto* $A \nsim \mathscr{P}(A)$.

El ejemplo anterior se puede generalizar a cualquier conjunto A no necesariamente finito.

Teorema 8.33. *Sea* A *un conjunto. Entonces* $A \nsim \mathscr{P}(A)$.

Prueba: Si $A = \varnothing$. Entonces $\mathscr{P}(A) = \{\varnothing\}$. Luego $|A| = 0$ y $|\mathscr{P}(A)| = 1$, luego por corolario anterior $A \nsim \mathscr{P}(A)$. Supongamos que $A \neq \varnothing$ y que $A \sim \mathscr{P}(A)$. Por tanto existe una función biyectiva $f : A \to \mathscr{P}(A)$. Tomemos $D := \{a \in A : a \notin f(a)\}$. Note que $D \subseteq A$ y por tanto $D \in \mathscr{P}(A)$. Como f es sobreyectiva existe $d \in A$ tal que $f(d) = D$. Ahora, supongamos que $d \in D$, entonces por definición de D, tenemos que $d \notin f(d) = D$, lo cual es absurdo. Si $d \notin D$. Entonces $d \in f(d) = D$, lo cual también es una contradicción y consecuentemente $A \nsim \mathscr{P}(A)$. □

Corolario 8.34. *$\mathscr{P}(\mathbb{N})$ es no-contable.*

Prueba: Como $\mathbb{N} \nsim \mathscr{P}(\mathbb{N})$, entones $\mathscr{P}(\mathbb{N})$ no es numerable. Falta probar que $\mathscr{P}(\mathbb{N})$ no es finito. Supongamos que $\mathscr{P}(\mathbb{N})$ es finito y defina $T = \{\{n\} : n \in \mathbb{N}\} \subseteq \mathscr{P}(\mathbb{N})$. Por Teorema 8.19 se tiene que T es finito, sin embargo, es evidente que $T \sim \mathbb{N}$, lo cual implica que $\mathbb{N}$ es finito. Por tanto $\mathscr{P}(\mathbb{N})$ es infinito. □

Teorema 8.35. *Para cada $n \in \mathbb{N}$, sea $I_n = [a_n, b_n]$, donde $a_n, b_n \in \mathbb{R}$, $a_n < b_n$. Si $I_{n+1} \subseteq I_n$ para cada $n \in \mathbb{N}$, entonces $\bigcap_{n\in\mathbb{N}} I_n \neq \varnothing$.*

Prueba: Definamos $E := \{a_n : n \in \mathbb{N}\}$. Como $E \neq \varnothing$ y está acotado superiormente, por ejemplo b_1 es una cota superior de E, entonces existe $x \in \mathbb{R}$ tal que $x = \sup E$. Luego $a_n \leq x$ para todo $n \in \mathbb{N}$. Ahora, sea $m \in \mathbb{N}$, entonces $a_m \leq a_{n+m} < b_{n+m} \leq b_n$ para todo $n \in \mathbb{N}$, así que b_n es una cota superior para E. Por tanto $x \leq b_n$ para todo $n \in \mathbb{N}$. En consecuencia $x \in I_n$ para todo $n \in \mathbb{N}$, luego $x \in \bigcap_{n\in\mathbb{N}} I_n$. □

La prueba del siguiente lema es dejada como ejercicio al lector.

Lema 8.36. *Si $a, b \in \mathbb{R}$, $a < b$ y $x \in \mathbb{R}$, entonces existen $c, d \in \mathbb{R}$ tales que $c < d$, $[c, d] \subseteq [a, b]$ y $x \notin [c, d]$.*

Teorema 8.37. *$[0, 1]$ es no-contable.*

Prueba: Supongamos que $[0, 1]$ es contable. La función $\varphi : \mathbb{N} \to [0, 1]$ dada por $\varphi(n) = 1/n$ es inyectiva, así que $\mathbb{N} \sim \varphi_*(\mathbb{N})$ y como $\mathbb{N}$ es infinito, entonces $\varphi_*(\mathbb{N})$ es infinito. Como $\varphi_*(\mathbb{N}) \subseteq [0, 1]$, tenemos que $[0, 1]$ es infinito y en consecuencia numerable. Sea $\psi : \mathbb{N} \to [0, 1]$ una función biyectiva y $x_i = \psi(i)$, para cada $i \in \mathbb{N}$. Luego $[0, 1] = \{x_1, x_2, x_3, ...\}$. Por el lema anterior podemos elegir $a_1 < b_1$ tales que $x_1 \in [a_1, b_1] \subseteq [0, 1]$. Después de elegir $a_1, b_1, ..., a_n, b_n$ tales que $a_k < b_k$ y $x_k \notin [a_k, b_k]$ para $k = 1, 2, ..., n$ y con la propiedad $[a_{k+1}, b_{k+1}] \subseteq [a_k, b_k]$ para $k = 1, 2, \ldots, n-1$, el lema anterior permite elegir $a_{n+1} < b_{n+1}$ tales que $x_{n+1} \notin [a_{n+1}, b_{n+1}] \subseteq [a_n, b_n]$. De esta manera, hemos definido inductivamente para cada $n \in \mathbb{N}$ un intervalo $I_n = [a_n, b_n]$ tal que $I_{n+1} \subseteq I_n$ y $x_n \notin I_n$ para todo $n \in \mathbb{N}$. Por Teorema 8.35 $\bigcap_{n\in\mathbb{N}} I_n \neq \varnothing$, así que podemos tomas $x \in \bigcap_{n\in\mathbb{N}} I_n$. Como

$$[0, 1] \cap \left(\bigcap_{n\in\mathbb{N}} I_n \right) = \varnothing,$$

entonces $x \notin [0, 1]$, lo cual es absurdo. □

Nota 8.38. (*i*) *Como* $[0,1] \subset \mathbb{R}$, *entonces* $\mathbb{R}$ *es no-contable.*

(*ii*) $\mathbb{I}$ *no es contable. Si* $\mathbb{I}$ *fuera contable, entonces* $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ *seria contable, lo cual es absurdo, así que* $\mathbb{I}$ *es no-contable.*

Un conjunto A se dice que tiene **menor cardinalidad** que un conjunto B, lo cual denotamos como $|A| < |B|$, si existe una función inyectiva de A en B que no es biyectiva de A en B. Si $|A| < |B|$ también escribimos $|B| > |A|$. Por ejemplo, como $\mathbb{N}$ es contable y $\mathbb{R}$ no lo es, no existe una funciíon biyectiva entre $\mathbb{N}$ y $\mathbb{R}$. Además, si definimos $f : \mathbb{N} \to \mathbb{R}$ como $f(n) = n$ se tiene que f es inyectiva y por tanto $|\mathbb{N}| < |\mathbb{R}|$. Adicionalmente, la notación $|A| \leq |B|$ significa que $|A| = |B|$ o $|A| < |B|$ (en este caso escribimos $|A| = |B|$ si $A \sim B$). Por tanto, para verificar que $|A| \leq |B|$ sólo tenemos que mostrar que existe una función inyectiva de A en B.

La cardinalidad de $\mathbb{N}$ la denotamos por $\aleph_0$ (que se lee aleph-cero), es decir, $|\mathbb{N}| = \aleph_0$. Lo que implica que si A es un conjunto contable, entonces $|A| = \aleph_0$. La cardinalidad del conjunto de los números reales es denotada por c, por tanto $|\mathbb{R}| = c$ y además $\aleph_0 < c$. Una conjetura interesante fue propuesta por Georg Cantor y es la siguiente.

Hipótesis del Continuo: No existe un conjunto S tal que $\aleph_0 < |S| < c$.

Si la Hipótesis de Continuo fuera cierta tendríamos que todo subconjunto no vacío de números reales sería contable o equipotente a los reales. Sin embargo, en 1931 Kurt Gödel probó que es imposible probar la negación de la Hipótesis del Continuo usando los axiomas de la Teoría de Conjuntos. En 1963, Paul Cohen mostró algo bien interesante también, que la Hipótesis del Continuo no puede ser *probada* usando estos mismos axiomas. Por tanto, la Hipótesis del Continuo es indepediente de los axiomas de la Teoría de Conjuntos.

Note que el Teorema 8.33 nos dice que si A es cualquier conjunto, entonces $|A| < |\mathscr{P}(A)|$. Por tanto se tiene la siguiente secuencia

$$\aleph_0 < c < |\mathscr{P}(\mathbb{R})| < |\mathscr{P}(\mathscr{P}(\mathbb{R}))| < |\mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{R})))| \cdots .$$

8.4. Ejercicios

1. Sean $m, n \in \mathbb{N}$. Si $J_m \sim J_n$, entonces $m = n$.

2. Sean $a, b \in \mathbb{R}$, $a < b$ y $x \in \mathbb{R}$. Muestre que existen $c, d \in \mathbb{R}$ tales que $c < d$, $[c, d] \subseteq [a, b]$ y $x \notin [c, d]$.

3. Sean A, B, C, D conjuntos tales que $A \cap B = \varnothing = C \cap D$, $A \sim C$ y $B \sim D$. Muestre que $A \cup B \sim C \cup D$.

4. Muestre que si $(A - B) \sim (B - A)$, entonces $A \sim B$.

5. Sean A, B y C conjuntos finitos. Muestre que

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

6. Sea $f : X \to Y$ una función inyectiva. Si Y es finito, muestre que X es finito y $|X| \leq |Y|$.

7. Sea $g : X \to Y$ una función sobreyectiva. Si X es finito, muestre que Y es finito y $|Y| \leq |X|$. (Sugerencia: Use el hecho que g tiene inversa a derecha si y sólo si g es sobreyectiva)

8. Sean $k \geq 2$ y $X_1, X_2, X_3, ..., X_k$ conjuntos finitos no vacíos, disjuntos dos a dos tales que $|X_i| = m_i$, para $i = 1, 2, 3, ..., k$. Entonces $\bigcup_{i=1}^{k} X_i$ es finito y $|\bigcup_{i=1}^{k} X_i| = \sum_{i=1}^{k} m_i$.

9. Sean $k \geq 2$ y $X_1, X_2, X_3, .., X_k$ conjuntos finitos no vacíos tales que $|X_i| = m_i$. Muestre que el producto cartesiano $\Pi_{i=1}^{k} X_i$ es finito y $|\Pi_{i=1}^{k} X_i| = m_1 m_2 m_3 \cdots m_k$.

10. Sean $n > 1$ y $\psi : J_n \to \mathbb{N}$ una función biyectiva. Definamos $\varphi : J_{n-1} \to \mathbb{N}$ por:

$$\varphi(k) = \begin{cases} \psi(k), & \text{si} \quad \psi(k) < \psi(n), \\ \psi(k) - 1, & \text{si} \quad \psi(k) > \psi(n). \end{cases}$$

Probar que φ es biyectiva.

11. Si E es un conjunto infinito, entonces E tiene un subconjunto numerable.

Sugerencia: Demuestre por inducción que para todo $n \in \mathbb{N}$, E tiene un subconjunto equipotente con J_n.

12. Si E es un conjunto, entonces E es infinito si y solo si E es equipotente a un subconjunto propio de E.

13. Sea A un conjunto numerable, muestre que $A \cup \{x\}$ es numerable.

14. Sea A un conjunto numerable y B un conjunto finito, muestre que $A \cup B$ es numerable.

15. Demostrar:

 a) Si E es un conjunto, entonces no existe una función sobreyectiva de E en $\mathscr{P}(E)$. En particular, si E es numerable, entonces $\mathscr{P}(E)$ es no contable.

 b) Si E es el conjunto de todas las funciones de $\mathbb{N}$ en $\{0, 1\}$, es decir, todas las sucesiones de ceros y unos, entonces E es no contable.

16. *Números Algebraicos y Trascendentes.* Un número real x se dice *algebraico* si existe un natural n, y enteros $a_0, a_1, \ldots, a_n$, $a_n \neq 0$, tal que

$$a_n x^n + \cdots + a_1 x + a_0 = 0.$$

Decimos que x es *trascendente* si no es algebraico. Probar que:

 a) El conjunto de los números algebraicos es contable.

 b) El conjunto de los números trascendentes es no contable.

17. Sea $f : [0,1] \to \mathbb{R}$. Supongamos que existe $M > 0$ tal que para toda elección finita de puntos $x_1, x_2, \ldots, x_n$ del intervalo $[0,1]$,

$$|f(x_1) + \cdots + f(x_n)| \leq M.$$

Probar que el conjunto $E := \{x \in [0,1] : f(x) \neq 0\}$ es contable.

18. Si A es un conjunto contable y B es un conjunto no contable, probar que $B \setminus A$ es equipotente a B.

19. Sea E el conjunto de todas las funciones de $\mathbb{R}$ en $\mathbb{R}$. Probar que $E \nsim \mathbb{R}$.

Sugerencia: Suponga que $E \sim \mathbb{R}$. Sea $f : \mathbb{R} \to E$ una fución biyectiva. Si $a \in \mathbb{R}$, sea $g_a := f(a)$ el elemento de E que corresponde al real a. Considere $h : \mathbb{R} \to \mathbb{R}$ definida por $h(x) = 1 + g_x(x)$ para $x \in \mathbb{R}$ y pruebe que $h \notin E$.

20. Sean X un conjunto no vacío y $f : \mathbb{N} \to X$ una función. Si $f_*(\mathbb{N})$ es finito, muestre que existe $x_0 \in f_*(\mathbb{N})$ tal que $f^*(\{x_0\})$ es infinito.

Capítulo 9

Los Números Complejos

El primer encuentro que tenemos con los números complejos es en la secundaria, cuando intentamos hallar raíces para las ecuaciones cuadráticas. En ese momento se introduce la unidad imaginaria $i = \sqrt{-1}$ y simplemente aprendemos a lidiar con ella de manera formal, entendiendo ciertas innovaciones que nos permiten hallar las raíces de cualquier ecuación de orden dos. En este capítulo, queremos ver los números complejos como un campo y familiarizarnos con aquellas nuevas propiedades que lo hacen diferente de los números reales. Los números complejos son una extensión de los reales y a diferencia de estos últimos contienen todas las raíces de cualquier polinomio sobre los reales o los complejos. Se cree que el primer matemático en usar los números complejos fue el italiano Girolamo Cardano (1501–1576) quien los utilizó en la fórmula que se tiene para resolver ecuaciones cúbicas. Las palabras "número complejo" fueron introducidas por el matemático alemán Carl Friedrich Gauss (1777–1855) quien uso los complejos en casi todas la áreas de la matemática desde el Ágebra hasta la Geometría No Euclidiana, lo que abrió el camino para el uso general y sistemático de estos nuevos números. En este capítulo sólo estaremos interesado en las propiedades algebraicas de los complejos, no estaremos interesado en su topología o temas de ese tipo, eso se hará en cursos más avanzados. Comenzaremos con unas definiciones básicas.

9.1. Álgebra de los Números Complejos

Consideremos la ecuación

$$x^2 + 1 = 0 \tag{9.1}$$

Supongamos que $t \in \mathbb{R}$ es solución de (9.1), entonces $t^2 + 1 = 0$, por lo tanto $t^2 = -1$. Si $t > 0$, entonces $t^2 > 0 > -1$. Si $t = 0 > -1$ y si $t < 0$, entonces $t^2 > 0 > -1$, en cualquier caso $t^2 \neq -1$. En consecuencia no hay un número real $x \in \mathbb{R}$ tal que $x^2 + 1 = 0$. Una solución para (9.1) seria un número i tal que $i^2 = -1$, como hemos visto anteriormente i no puede ser real.

En este punto vale la pena recordar que $\mathbb{R}^2$ es el conjunto de todas las parejas de números reales (a, b) que satisfacen $(a, b) = (c, d)$ si y sólo si $a = c$ y $b = d$. Lo que haremos será dotar a $\mathbb{R}^2$ de una estructura de campo escogiendo de forma adecuada la suma y la multiplicación. Definiremos la

suma de (a, b) y (c, d) como la pareja

$$(a, b) + (c, d) = (a + c, b + d).$$

El producto de las parejas anteriores se define como

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Definición 9.1 (Números Complejos)**.** *El conjunto de los números complejos, el cual denotamos por* $\mathbb{C}$*, se define como* $\mathbb{R}^2$ *dotado de las operciones suma y multiplicación dadas anteriormente.*

Es fácil ve que $\mathbb{C}$ es un campo, donde la unidad aditiva es $(0, 0)$ y la unidad multiplicativa es $(1, 0)$. El inverso aditivo de (a, b) es $(-a, -b)$ y si $(a, b) \neq (0, 0)$ su inverso multiplicativo es $(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2})$. Como veremos de aquí en adelante $\mathbb{C}$ es estructuralmente más rico que $\mathbb{R}^2$. Los elementos de $\mathbb{C}$ los llamaremos números complejos.
Consideremos la funcón $H : \mathbb{R} \to \mathbb{C}$ definida por $H(x) = (x, 0)$. Esta función es un monomorfismo, es decir,

- H es inyectiva
- $H(x + y) = H(x) + H(y)$, $H(xy) = H(x) \cdot H(y)$
- $H(0) = (0, 0)$ y $H(1) = (1, 0)$.

De aquí en adelante identificaremos a cada elemento $x \in \mathbb{R}$ con $H(x) = (x, 0)$, en particular, 0 será indentificado con $H(0) = (0, 0)$ y 1 con $H(1) = (1, 0)$. Denotaremos por i al número complejo $(0, 1)$. Con estas convenciones, se tiene que para reales x, y

$$(x, y) = x + iy.$$

En efecto $x + iy = (a, 0) + (0, 1)(y, 0) = (x, 0) + (0, y) = (x, y)$. La expresión $a + bi$ se llama forma normal de un número complejo. Al número real a se le llama parte real de $a + bi$ y lo denotamos $a = \mathrm{Re}(a + bi)$. Al número real b se le llama parte imaginaria de $a + bi$ y lo denotamos por $b = \mathrm{Im}(a + bi)$.

La igualdad en los complejos es la misma que en $\mathbb{R}^2$, sin embargo vale la pena observar como queda ésta con la identificación hecha arriba.

Definición 9.2 (Igualdad de Complejos)**.** *Decimos que dos números complejos* $a + bi$ *y* $c + di$ *son iguales, y escribimos* $a + bi = c + di$*, si* $a = c$ *y* $b = d$*.*

Nota 9.3. *Dados* $z, w \in \mathbb{C}$*, en lugar de* $z + (-w)$ *escribimos* $z - w$*. Muchas veces también escribimos* zw *en vez de* $z \cdot w$*.*

A continuación enunciamos algunas consecuencias para los números complejos que se tiene por ser $\mathbb{C}$ un campo, la prueba es dejada como ejercicio.

Proposición 9.4. *Si* $z, w, y \in \mathbb{C}$*, entonces*

(*i*) $z \cdot 0 = 0$

(*ii*) $-z = (-1)z$

(*iii*) $z(-y) = (-z)y = -(zy)$

(*iv*) $(-z)(-y) = zy$

(*v*) *Si* $z \cdot y = 0$, *entonces* $z = 0$ *ó* $y = 0$

(*vi*) *Si* $z + y = z + w$, *entonces* $y = w$

(*vii*) *Si* $zy = zw$, $z \neq 0$, *entonces* $y = w$

(*viii*) *Si* $z \neq 0$, *entonces* $(z^{-1})^{-1} = z$.

Definición 9.5. *Sean* $z, w \in \mathbb{C}$, *con* $w \neq 0$. *Se define el cociente de* z *y* w, *denotado* z/w *o* $\frac{z}{w}$, *como*

$$z/w = z \cdot w^{-1}$$

De la definición se deduce que $z^{-1} = 1 \cdot z^{-1} = \dfrac{1}{z}$.

Proposición 9.6. *Si* $z_1, z_2, z_3, z_4 \in \mathbb{C}$, *con* $z_2 \neq 0$ *y* $z_4 \neq 0$, *entonces*

(*i*) $(z_2 z_4)^{-1} = z_2^{-1} z_4^{-1}$

(*ii*) $\dfrac{z_1}{1} = z_1$

(*iii*) $\dfrac{z_1}{z_2} \cdot \dfrac{z_3}{z_4} = \dfrac{z_1 \cdot z_3}{z_2 \cdot z_4}$

(*iv*) $\dfrac{z_1}{z_2} + \dfrac{z_3}{z_2} = \dfrac{z_1 + z_3}{z_2}$

(*v*) $\dfrac{z_1}{z_2} + \dfrac{z_3}{z_4} = \dfrac{z_1 z_4 + z_2 z_3}{z_2 z_4}$

(*vi*) *Si* $z_3 \neq 0$, $\dfrac{\dfrac{z_1}{z_2}}{\dfrac{z_3}{z_4}} = \dfrac{z_1 z_4}{z_2 z_3}$

(*vii*) $\left(\dfrac{z_2}{z_4}\right)^{-1} = \dfrac{z_4}{z_2}$

(*viii*) $-\dfrac{z_2}{z_4} = \dfrac{-z_2}{z_4} = \dfrac{z_2}{-z_4}$

De igual forma como se definió potencias en un campo F se define en $\mathbb{C}$ así,

Definición 9.7. *Dados* $n \in \mathbb{N}$ *y* $z \in \mathbb{C}$, *definimos* $z^1 = z$ *y* $z^{n+1} = z^n \cdot z$. *Si* $z \neq 0$, *definimos* $z^{-n} = (z^{-1})^n$ *y* $z^0 = 1$.

9.2. Complejos Conjugados. Módulo de Complejos

Definición 9.8. *Sea* $a + bi$ *un número complejo.*

(*i*) *Definimos el conjugado de* $a + bi$, *denotado* $\overline{a + bi}$, *como* $\overline{a + bi} = a - bi$

(*ii*) *Definimos el valor absoluto o módulo de* $a + bi$, *denotado por* $|a + bi|$, *como la raíz cuadrada del número real* $a^2 + b^2$, *es decir,*

$$|a + bi| = \sqrt{a^2 + b^2}$$

Nota 9.9. *Si* $z = a + bi$, *entonces* $z \cdot \overline{z} = (a + bi)(a - bi) = a^2 + b^2$, *lo que implica que* $|z|^2 = z \cdot \overline{z}$. *Por lo tanto* $|z| = \sqrt{z \cdot \overline{z}}$.

Proposición 9.10. *Si* w *y* z *son números complejos, entonces:*

(*i*) $\overline{(\overline{z})} = z$

(*ii*) $\overline{z+w} = \overline{z} + \overline{w}$

(*iii*) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$

(*iv*) $\overline{z-w} = \overline{z} - \overline{w}$

(*v*) *Si* $z \neq 0$, *entonces* $\overline{\left(\frac{w}{z}\right)} = \frac{\overline{w}}{\overline{z}}$.

Prueba: Sólo demostraremos (*ii*), el resto de la prueba es dejado al lector. Sean $z = a + bi$ y $w = c + di$. Entonces

$$\overline{z+w} = \overline{(a+bi)+(c+di)} = \overline{(a+c)+(b+d)i} = (a+c)-(b+d)i = (a-bi)+(c-di) = \overline{z}+\overline{w}.$$

□

Proposición 9.11. *Si w y z son números complejos, entonces:*

(*i*) $|z| = 0$ *si y sólo si* $z = 0$.

(*ii*) $|\overline{z}| = |z|$.

(*iii*) $|zw| = |z||w|$.

(*iv*) $|z+w| \leq |z| + |w|$.

(*v*) *Si* $z \neq 0$, *entonces* $|w/z| = |w|/|z|$.

(*vi*) $|z| - |w| \leq |z-w|$.

Prueba: Sólo mostraremos (*iv*), el resto de la prueba es dejada al lector. Note que

$$|z+w|^2 = (z+w)\overline{(z+w)} = (z+w)(\overline{z}+\overline{w}) = |z|^2 + z\overline{w} + \overline{z}w + |w|^2.$$

Observe que $\overline{z}w = \overline{z\overline{w}}$ y además que para cualquier complejo z se tiene que $z + \overline{z} = 2\mathrm{Re}z$. Por tanto

$$|z+w|^2 = |z|^2 + 2\mathrm{Re}(z\overline{w}) + |w|^2.$$

Note también que para cualquier complejo α se tiene que $\mathrm{Re}z \leq |\mathrm{Re}z| \leq |z|$. De donde se sigue que

$$|z+w|^2 \leq |z|^2 + 2|z\overline{w}| + |w|^2 = |z|^2 + 2|z||\overline{w}| + |w|^2 = (|z| + |w|)^2.$$

Lo que muestra el resultado deseado. □

Ejemplo 9.12. *Hallar el módulo del complejo* $z = \frac{(4+3i)(1+i)}{1-7i}$

Solución:

$$|z| = \frac{|4+3i||1+i|}{|1-7i|} = \frac{\sqrt{25}\sqrt{2}}{\sqrt{50}} = 1.$$

Nota 9.13. *Vale la pena notar que no es posible definir un orden en los complejos que sea compatible con su estructura algebraica. Para mostrar esto, razonemos por el absurdo y asumamos que hemos posido definir un orden el los complejos que denotamos por* $\ll$, *luego* $\ll$ *satisface tricotomía, transitividad y monotonía de la suma y el producto. Como* $i \neq 0$, *se tiene que* $0 \ll i^2 = -1$. *Entonces* $0 \ll -1$ *y de igual forma se muestra que* $0 \ll 1$. *Por tanto,* $0 \ll -1+1 = 0$, *lo cual es absurdo, pues* $0 = 0$.

9.3. Raíces Cuadradas de un Complejo

Encontrar las raíces cuadradas de un complejo z equivale a resolver la ecuación $X^2 - z = 0$. El algoritmo para resolver la ecuación antes mecionada está expresado en el siguiente resultado.

Proposición 9.14. *Sea $z = a + bi$ un número complejo, entonces:*

(i) Si $b > 0$, las dos raíces de la ecuación $X^2 = a + bi$ vienen dadas por

$$X = \pm\left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\right)$$

(ii) Si $b < 0$, las dos raíces de la ecuación $X^2 = a + bi$ vienen dadas por

$$X = \pm\left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} - i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\right)$$

(iii) Si $b = 0$, la ecuación $X^2 = a + bi$, se reduce $X^2 = a$, cuyas raíces son:

(a) Si $a \geq 0$, $X = \pm\sqrt{a}$.

(b) Si $a < 0$, $X = \pm i\sqrt{-a}$.

Prueba: Sea $X = x + yi$, entonces por hipótesis $(x + yi)^2 = a + bi$, de donde se sigue que $x^2 + 2xyi - y^2 = a + bi$. Por igualdad de complejos se obtiene

$$x^2 - y^2 = a \quad \text{y} \quad 2xy = b.$$

Como $(x^2 + y^2)^2 = (x^2 - y^2)^2 + 4x^2y^2$, entonces $(x^2 + y^2)^2 = a^2 + b^2$ y como $x^2 + y^2 \geq 0$, se tiene que

$$x^2 + y^2 = \sqrt{a^2 + b^2}.$$

Como $x^2 - y^2 = a$, entonces $x^2 = a + y^2$, luego $2y^2 = \sqrt{a^2 + b^2} - a$, de lo que se obtiene

$$y = \pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}$$

Además $y^2 = x^2 - a$, entonces $x^2 + x^2 - a = \sqrt{a^2 + b^2}$. Luego

$$x = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}.$$

Como $2xy = b$, entonces los signos de x e y dependen de b. Si $b > 0$, entonces $x > 0$ y $y > 0$ ó $x < 0$ y $y < 0$. Si $b < 0$, entonces $x < 0$ y $y > 0$ ó $x > 0$ y $y < 0$. □

Nota 9.15. *Si x_1 es una raíz cuadrada de un complejo $z \neq 0$, entonces $-x_1$ también lo es. Luego las raíces de la ecuación cuadrática $Ax^2 + Bx + C = 0$, donde A, B y C son números complejos, vienen dadas por:*

$$x = \frac{-B \pm W}{2A},$$

donde W es una raíz de la ecuación $y^2 = B^2 - 4AC$.

Ejemplo 9.16. *Encontrar las raíces cuadradas de $z = 4 + 3i$.*

Solución: Basta resolver la ecuación $x^2 = 4 + 3$. En este caso $a = 4$ y $b = 3 > 0$. Luego

$$\begin{aligned} x &= \pm \left(\sqrt{\frac{\sqrt{16+9}+4}{2}} + i\sqrt{\frac{\sqrt{16+9}-4}{2}} \right) \\ &= \pm \left(\frac{3}{\sqrt{2}} + i\frac{1}{\sqrt{2}} \right) \end{aligned}$$

Ejemplo 9.17. *Resolver la ecuación $x^2 - (1+i)x + (6-2i) = 0$.*

Solución: En este caso en $A = 1$, $B = -(1+i)$ y $C = 6 - 2i$. Luego las raíces vienen dadas por

$$x = \frac{(1+i) \pm W}{2}$$

donde W es la raíz de $y^2 = -24 + 10i$. Pero

$$y = \pm \left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} \right)$$

Luego $W = 1 + 5i$, $-w = -(1+5i)$. Así que

$$x_1 = \frac{(1+i)+(1+5i)}{2} = 1 + 3i \quad \text{y} \quad x_2 = -2i$$

Nota 9.18. *Como es sabido en los reales la ecuación $x^2 = y$, con y un real positivo, tiene dos soluciones. En este caso escogimos la solución positiva y la llamamos la raíz de y. Todas las propiedades usuales de la radicación se satisfacian sin ningún problema. Lo anterior no sucede en los complejos. No importa cual raíz se escoja, las propiedades de la radicación no se satisfacen en general, en los ejercicios invitamos al estudiante a comprobarlo. La misma observación aplica para las raices n-ésimas, es decir para la soluciones de la ecuación $x^n = y$.*

9.4. Forma Trigonométrica de un Complejo

Considere z un complejo diferente de cero. Siempre es posibles expresar z en su *forma polar*,

$$z = |z|(\cos\theta + i\sin\theta), \tag{9.2}$$

donde θ es un número real: si $z = x + iy$, simplemente escoja cualquier θ tal que $\cos(\theta) = x/|z|$ y $\text{sen}(\theta) = y/|z|$. Por ejemplo $1 + i$ tiene la representación polar

$$1 + i = \sqrt{2}(\cos(\pi/4) + i\ \text{sen}(\pi/4)).$$

Cada número real θ para el cual se satisface (9.2) es llamado un *argumento* de z. Geométricamente, θ proporciona la medida en radianes del ángulo medido desde el eje positivo real a el vector que representa a z en el plano complejo.

Como para todo $m \in \mathbb{Z}$

$$\begin{aligned}\cos(2m\pi + \alpha) &= \cos\alpha \\ \sin(2m\pi + \alpha) &= \sin\alpha\end{aligned}$$

entonces $\arg z$ puede tomar muchos valores, por tanto $\arg z$ es en realidad un conjunto. Si asumimos que uno de los argumentos de z es conocido, digamos θ_0, entonces

$$\arg z = \{\theta_0 + 2k\pi : k \ \text{ es un entero}\}.$$

Por tanto, es conveniente tomar un miembro especial de este conjunto, el único argumento θ de z en $-\pi < \theta \leq \pi$, en este caso θ es llamado argumento principal de z y por simplicidad, lo denotaremos como Argz.

Dado $z = x + iy$, con $z \neq 0$, podemos determinar el argumento de z de la siguiente forma: primero determinamos el ángulo w tal que $w = \text{Arcsen}\,(y/|z|)$. Luego

(*i*) Si $x \geq 0$, elegimos $\theta = w$

(*ii*) Si $x < 0$ y $y < 0$, elegimos $\theta = -\pi - w$

(*iii*) Si $x < 0$ y $y \geq 0$, elegimos $\theta = \pi - w$.

Aquí, para cada t en $[-1, 1]$, Arsen(t) es el único número u en $[\pi/2, \pi/2]$ tal que $\text{sen}(u) = t$.

Ejemplo 9.19. *Exprese en forma trigonométrica los siguientes los números complejos* $z = -3$, $z = 7i$ *y* $z = -8 - 8\sqrt{3}i$.

Solución:

(*i*) $z = -3$. En este caso $r = |z| = 3$ y $y = 0$, luego $w = \text{Arcsen}(0) = 0$, así que $\theta = \pi - 0 = \pi$, entonces $z = 3(\cos(\pi) + i\ \text{sen}(\pi))$

(*ii*) $z = 7i$. En este caso $r = |z| = 7$ y $y = 7$, luego $w = \text{Arcsen}(1) = \pi/2$, lo que implica que $\theta = \frac{\pi}{2}$, entonces $z = 7[\cos(\frac{\pi}{2}) + i\ \text{sen}(\frac{\pi}{2})]$

(*iii*) $z = -8 - 8\sqrt{3}i$. En este caso $r = |z| = 16$ y $y = -8\sqrt{3}$, luego $w = \text{Arcsen}(-\sqrt{3}/2) = -2\pi/3$, entonces $\theta = -\pi - \frac{2\pi}{3} = -\frac{5\pi}{3}$, así que $z = 16[\cos(\frac{-5\pi}{3}) + i\ \text{sen}(\frac{-5\pi}{3})]$.

9.5. Fórmula de Moivre

Sean $z_1 = r_1(\cos\theta_1 + i\ \text{sen}\theta_1)$ y $z_2 = r_2(\cos\theta_2 + i\ \text{sen}\theta_2)$. Entonces

$$\begin{aligned} z_1 \cdot z_2 =& r_1 r_2(\cos\theta_1 + i\ \text{sen}\theta_1)(\cos\theta_2 + i\ \text{sen}\theta_2) \\ =& r_1 r_2[(\cos\theta_1\cos\theta_2 - \text{sen}\theta_1\text{sen}\theta_2) + i(\cos\theta_1\text{sen}\theta_2 + i\ \text{sen}\theta_1\cos\theta_2)] \\ =& r_1 r_2[\cos(\theta_1+\theta_2) + i\ \text{sen}(\theta_1+\theta_2)] \end{aligned}$$

Luego

$$z_1 \cdot z_2 = r_1 r_2[\cos(\theta_1+\theta_2) + i\ \text{sen}(\theta_1+\theta_2)].$$

De forma inductiva se muestra que

$$z_1 \cdot z_2 \cdots z_n = r_1 \cdot r_2 \cdots r_n[\cos(\theta_1+\theta_2+\cdots+\theta_n) + i\ \text{sen}(\theta_1+\theta_2+\cdots+\theta_n)]$$

Por tanto si $|z| = r$ y $\theta = \text{Arg}z$, entonces

$$z^n = r^n[\cos(n\theta) + i\ \text{sen}(n\theta)]. \tag{9.3}$$

Si tomamos $|z| = 1$, entonces $z = \cos\theta + i\ \text{sen}\theta$ y en consecuencia

$$z^n = \cos(n\theta) + i\ \text{sen}(n\theta)$$

Usando la fórmula (9.3) se sigue la importante identidad conocida como Fórmula de Moivre:

$$(\cos\theta + i\ \text{sen}\theta)^n = \cos(n\theta) + i\ \text{sen}(n\theta),\ \text{para todo}\ \ n \in \mathbb{N}.$$

Ahora suponga que $z_2 \neq 0$, entonces

$$\begin{aligned} \frac{z_1}{z_2} =& \frac{r_1(\cos\theta_1 + i\ \text{sen}\ \theta_1)}{r_2(\cos\theta_2 + i\ \text{sen}\ \theta_2)} = \frac{r_1(\cos\theta_1 + i\ \text{sen}\ \theta_1)(\cos\theta_2 - i\ \text{sen}\ \theta_2)}{r_2(\cos\theta_2 + i\ \text{sen}\ \theta_2)(\cos\theta_2 - i\ \text{sen}\ \theta_2)} \\ =& \frac{r_1}{r_2}\left[\frac{(\cos\theta_1\cos\theta_2 + \text{sen}\ \theta_1\text{sen}\ \theta_2) + i(-\cos\theta_1\text{sen}\ \theta_2 + \text{sen}\ \theta_1\cos\theta_2)}{\cos^2\theta_2 + \text{sen}^2\ \theta_2}\right] \end{aligned}$$

Luego

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\theta_1-\theta_2) + i\ \text{sen}(\theta_1-\theta_2)].$$

Note que

$$\frac{1}{\cos\theta + i\ \text{sen}\ \theta} = \frac{\cos(0) + i\ \text{sen}(0)}{\cos\theta + i\ \text{sen}\ \theta} = \cos(-\theta) + i\ \text{sen}(-\theta).$$

Entonces $(\cos\theta + i\ \text{sen}\ \theta)^{-1} = \cos(-\theta) + i\,\text{sin}(-\theta)$ y además

$$(\cos\theta + i\ \text{sen}\ \theta)^{-n} = [(\cos\theta + i\ \text{sen}\ \theta)^{-1}]^n = [\cos(-\theta) + i\ \text{sen}(-\theta)]^n = \cos(-n\theta) + i\ \text{sen}(-n\theta).$$

Luego se tiene la Fórmula de Moivre:

$$(\cos\theta + i\ \text{sen}\ \theta)^m = \cos(m\theta) + i\ \text{sen}(m\theta),\ \text{para todo}\ m \in \mathbb{Z}.$$

9.6. Resolución de la Ecuación $x^n - z = 0$

Veremos enseguida que la ecuación

$$x^n - z = 0 \tag{9.4}$$

donde $z \in \mathbb{C}$, $z \neq 0$ y $n \in \mathbb{N}$, es soluble en $\mathbb{C}$ y que tiene exactamente n-soluciones (o raíces distintas). Para eso usaremos el siguiente teorema de Teoría de Números, el cual ya fue probado en los ejercicios del Capítulo 7.

Teorema 9.20 (Algoritmo de la División). *Si $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces existen $q, r \in \mathbb{Z}$ únicos, tales que*

$$a = bq + r, \quad con \quad 0 \leq r < |b|.$$

Para hallar las raíces de $x^n - z = 0$, considere $\theta = \text{Arg} z$,

$$z = r(\cos\theta + i \text{ sen } \theta) \text{ y } x = R(\cos\varphi + i \text{ sen } \varphi).$$

Luego

$$(R(\cos\varphi + i \text{ sen } \varphi))^n = r(\cos\theta + i \text{ sen } \theta).$$

Entonces usando la Fórmula de Moivre se tiene que

$$R^n(\cos(n\varphi) + i\sin(n\varphi)) = r(\cos\theta + i\sin\theta).$$

Por igualdad de complejos $R^n = r$ y $n\varphi = \theta + 2k\pi$, con $k \in \mathbb{Z}$. Por lo tanto $R = \sqrt[n]{r}$ y $\varphi = \dfrac{\theta + 2k\pi}{n}$, $k \in \mathbb{Z}$. En resumen

$$x = \sqrt[n]{r}\left[\cos\left(\frac{\theta + 2k\pi}{n}\right) + i \text{ sen}\left(\frac{\theta + 2k\pi}{n}\right)\right], \quad k \in \mathbb{Z}.$$

Ahora veremos que el número de soluciones distintas de (9.4) es n. En efecto, como $k \in \mathbb{Z}$ y $n \in \mathbb{N}$, por el Teorema 9.20 existen $q, l \in \mathbb{Z}$ con $0 \leq l < n$ tales que: $k = nq + l$. Entonces

$$\frac{\theta + 2k\pi}{n} = \frac{\theta + 2(nq + l)\pi}{n} = \frac{\theta + 2l\pi}{n} + 2q\pi.$$

Por lo tanto

$$\cos\left(\frac{\theta + 2k\pi}{n}\right) = \cos\left(\frac{\theta + 2l\pi}{n}\right) \text{ y } \text{sen}\left(\frac{\theta + 2k\pi}{n}\right) = \text{sen}\left(\frac{\theta + 2l\pi}{n}\right).$$

Lo anterior dice que para todo $k \in \mathbb{Z}$, existe $l \in \{0, 1, \cdots, n-1\}$ tal que

$$\cos\left(\frac{\theta + 2k\pi}{n}\right) + i \text{ sen}\left(\frac{\theta + 2k\pi}{n}\right) = \cos\left(\frac{\theta + 2l\pi}{n}\right) + i \text{ sen}\left(\frac{\theta + 2l\pi}{n}\right)$$

Por tanto a lo sumo hay n-soluciones distintas de (9.4).
Ahora, considere $k_1, k_2 \in \{0, 1, \cdots, n-1\}$ con $k_1 \neq k_2$ y consideremos

$$x_{k_1} = \sqrt[n]{r}\left[\cos\left(\frac{\theta + 2k_1\pi}{n}\right) + i \text{ sen}\left(\frac{\theta + 2k_1\pi}{n}\right)\right] \quad \text{y}$$

$$x_{k_2} = \sqrt[n]{r}\left[\cos\left(\frac{\theta+2k_2\pi}{n}\right) + i\ \text{sen}\left(\frac{\theta+2k_2\pi}{n}\right)\right].$$

Si $x_{k_1} = x_{k_2}$, entonces existe $s \in \mathbb{Z}$ tal que

$$\frac{\theta+2k_1\pi}{n} = \frac{\theta+2k_2\pi}{n} + 2s\pi.$$

Luego $\theta + 2k_1\pi = \theta + 2k_2\pi + 2sn\pi$ y consecuentemente $k_1 - k_2 = ns$, lo cual es imposible ya que $0 \leq k_1 \leq n-1$ y $0 \leq k_2 \leq n-1$ luego $-(n-1) \leq k_1 - k_2 \leq (n-1)$. Así al sustituir $k = 0, 1, \cdots, n-1$ en (9.4) se obtiene una solución distinta de (9.4).

Teorema 9.21. *Todas las soluciones de $x^n = r(\cos\theta + i\ sen\ \theta)$, ($r > 0$ y $\theta = \text{Arg}z$) vienen dadas por*

$$x_k = \sqrt[n]{r}\left[\cos\left(\frac{\theta+2k\pi}{n}\right) + i\ sen\left(\frac{\theta+2k\pi}{n}\right)\right], \text{ donde } \ k = 0, 1, \cdots, n-1. \tag{9.5}$$

Además, si $k_i \neq k_j$, entonces $x_{k_i} \neq x_{k_j}$.

La $n-$ésima raíz de z obtenida al hacer $k = 0$ en la ecuación (9.5) es llamada la $n-$ésima raíz principal de z. La notación $\sqrt[n]{z}$ está reservada para esta raíz especial, lo cual es consistente con la notación $\sqrt[n]{r}$ en la ecuación (9.5), la cual indica la única raíz real de $r = |z|$. Como (9.5) no es válida para $z = 0$, acordamos que $\sqrt[n]{0} = 0$ y además $\sqrt[2]{z} = \sqrt{z}$.

Ejemplo 9.22. *Resolver $x^3 = 8i$.*

Solución: Note que $8i = 8\left[\cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right)\right]$, entonces $x_0 = \sqrt{3} + i$, $x_1 = -\sqrt{3} + i$ y $x_0 = -2i$.

9.7. Representación Geométrica de las Raíces

Si $z = r(\cos\theta + i\sin\theta)$, con $\theta = \text{Arg}z$, entonces las raíces de la ecuación $x^n - z = 0$ vienen dadas por

$$x = \sqrt[n]{r}\left[\cos\left(\frac{\theta+2k\pi}{n}\right) + i\sin\left(\frac{\theta+2k\pi}{n}\right)\right].$$

Así que todas tienen módulo $\sqrt[n]{r}$, es decir, se encuentran en la circunferencia de radio $R = \sqrt[n]{r}$ y centro en el origen. Además el ángulo entre dos raíces consecutivas es

$$\frac{\theta+2(j+1)\pi}{n} - \frac{\theta+2j\pi}{n} = \frac{2\pi}{n}.$$

Como son n raíces, entonces son n ángulos y por lo tanto la suma de sus medidas es 2π. Así que geométricamente las raíces parten a la circunferencia de radio $R = \sqrt[n]{r}$ y centro en el origen en n arcos iguales.

Ejemplo 9.23. *Representar las raíces de $x^3 = 8i$ las cuales son: $x_0 = \sqrt{3} + i$, $x_1 = -\sqrt{3} + i$ y $x_0 = -2i$.*

9.8. Las Raíces n-ésimas de la Unidad.

Encontrar las raíces n-ésimas de la unidad, significa encontrar la solución de la ecuación

$$x^n - 1 = 0.$$

Como $1 = \cos 0 + i \text{ sen } 0$, entonces

$$x_k = \cos\left(\frac{2k\pi}{n}\right) + i \text{ sen}\left(\frac{2k\pi}{n}\right),$$

con $k = 0, 1, \cdots, n-1$. Por la fórmula de Moivre tenemos que

$$\cos\left(\frac{2k\pi}{n}\right) + i \text{ sen}\left(\frac{2k\pi}{n}\right) = \left[\cos\left(\frac{2\pi}{n}\right) + i \text{ sen}\left(\frac{2\pi}{n}\right)\right]^k.$$

Luego

$$x_k = \left[\cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)\right]^k,$$

con $k \in \{0, 1, 2, ..., n-1\}$. Las raíces son precisamente $w^0, w, w^2, \cdots, w^{n-1}$, donde

$$w = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right).$$

Lo anterior se puede emplear para resolver la ecuación

$$x^m + x^{m-1} + \cdots + x + 1 = 0.$$

En efecto: Claramente

$$x^{m+1} - 1 = (x-1)(x^m + x^{m-1} + \cdots + x + 1).$$

Como $1 = w^0, w, w^2, \cdots, w^m$ son las raíces de $x^{m+1} - 1 = 0$, entonces

$$0 = (w^k)^{m+1} - 1 = (w^k - 1)[(w^k)^m + (w^k)^{m-1} + \cdots + (w^k) + 1],$$

para $k = 0, 1, \cdots, m$. Si $k \geq 1$, entonces $w^k \neq 1$, luego

$$(w^k)^m + (w^k)^{m-1} + \cdots + (w^k) + 1 = 0,$$

para todo $k = 1, 2, \cdots, m$. Por tanto $w, w^2, \cdots, w^m$ son raíces de

$$x^m + x^{m-1} + \cdots + x + 1 = 0.$$

Y son todas ya que si hubiera otra diferente de ellas, entonces también lo seria de $x^{m+1} - 1 = 0$, lo que no es posible.

En conclusion para resolver la ecuación $x^m + x^{m-1} + \cdots + x + 1 = 0$ basta resolver $x^{m+1} - 1 = 0$ cuyas raíces son $w^0, w, w^2, \cdots, w^m$ donde

$$w = \cos\left(\frac{2\pi}{m+1}\right) + i \text{ sen}\left(\frac{2\pi}{m+1}\right)$$

y de éstas $w, w^2, \cdots, w^m$ son las raíces de $x^m + x^{m-1} + \cdots + x + 1 = 0$.

Ejemplo 9.24. *Resolver la ecuación* $x^3 + x^2 + x + 1 = 0$.

Solución: Basta resolver $x^4 - 1 = 0$ cuyas raíces vienen dados por

$$x = \cos\left(\frac{2k\pi}{4}\right) + i \operatorname{sen}\left(\frac{2k\pi}{4}\right),$$

donde $k = 0, 1, 2, 3$. Substituyendo k se tiene que $x_0 = 1, x_1 = i, x_2 = -1$ y $x_3 = -i$. Así las raíces de $x^3 + x^2 + x + 1$ son $i, -1$ y $-i$.

9.9. Ejercicios

1. Sea $z \in \mathbb{C}$, pruebe que

 a) $\overline{z^n} = (\overline{z})^n$, para todo $n \in \mathbb{N}$.

 b) Si $z \neq 0$, entonces $\overline{z^{-1}} = (\overline{z})^{-1}$.

 c) Si $z \neq 0$, entonces $\overline{z^{-n}} = (\overline{z})^{-n}$, para todo $n \in \mathbb{N}$.

 d) $|z^n| = |z|^n$, para todo $n \in \mathbb{N}$.

 e) Si $z \neq 0$, entonces $|z^{-1}| = |z|^{-1}$.

 f) Si $z \neq 0$, entonces $|z^{-n}| = |z|^{-n}$, para todo $n \in \mathbb{N}$.

2. Muestre que $\arg(z^{-1}) = -\arg z$ y $\arg(zw) = \arg z + \arg w$. Sin embargo, en general no es cierto que $\operatorname{Arg}(z^{-1}) = -\operatorname{Arg} z$ y $\operatorname{Arg}(zw) = \operatorname{Arg} z + \operatorname{Arg} w$.

3. Muestre que si z es un complejo no nulo, entonces

$$\operatorname{Arg}(z) = \begin{cases} 2\arctan\left(\frac{\operatorname{Im} z}{\operatorname{Re} z + |z|}\right), & \text{si } z \notin \mathbb{R}^- \\ \pi, & \text{si } x \in \mathbb{R}^-. \end{cases}$$

 Aquí $\mathbb{R}^-$ denota los números reales negativos.

4. Si $|z| = 3$ ¿Cuál es el valor máximo que puede tomar $|1 + z + z^3|$?

5. Muestre que si $z = \overline{z}$, entonces $z \in \mathbb{R}$.

6. Sean z, w complejos. Muestre que $|z| - |w| \leq |z + w|$ y $||z| - |w|| \leq |z \pm w|$.

7. Resuelva las siguientes ecuaciones:

 a) $x^2 - 1 - \sqrt{3}i = 0$.

 b) $x^2 + 2ix - 1 = 0$.

 c) $x^2 - (2 + 3i)x - 1 + 3i = 0$.

 d) $ix^6 + 4i = 0$.

 e) $x^5 + x^4 + x^3 + x^2 + x = 0$.

8. Muestre la llamada Ley del Paralelogramo para los complejos z, w, esto es,

$$|z+w|^2 + |z-w|^2 = 2|z|^2 + 2|w|^2.$$

9. Dados $z \neq 0$ y $w \neq 0$, muestre que $|z+w| = |z| + |w|$ si y sólo si $w = tz$ para algún $t > 0$.

10. Sea c un número complejo tal que $|c| < 1$. Muestre que $|z+c| \leq |1 + \overline{c}z|$ si y sólo si $|z| \leq 1$. ¿Cuándo se tiene la igualdad?

11. Muestre la identidad de Lagrange: Para $z_1, z_2, \cdots, z_n$ y $w_1, w_2, \cdots, w_n$ en $\mathbb{C}$,

$$\left|\sum_{k=1}^{n} z_k w_k\right|^2 = \left(\sum_{k=1}^{n} |z_k|^2\right)\left(\sum_{k=1}^{n} |w_k|^2\right) - \sum_{1\leq k<j\leq n} |z_k\overline{w}_j - z_j\overline{w}_k|^2 .$$

Usando el resultado anterior, pruebe que

$$\left|\sum_{k=1}^{n} z_k w_k\right| \leq \left(\sum_{k=1}^{n} |z_k|^2\right)^{\frac{1}{2}}\left(\sum_{k=1}^{n} |w_k|^2\right)^{\frac{1}{2}}.$$

12. Muestre que $|\mathrm{Re}z|, |\mathrm{Im}z| \leq |z|$ y $|z| \leq |\mathrm{Re}z| + |\mathrm{Im}z| \leq \sqrt{2}|z|$.

13. Escribiendo $z = \cos\theta + i\mathrm{sen}\theta$ en la identidad

$$1 + z + z^2 + \cdots + z^{n-1} = \frac{1-z^n}{1-z},$$

muestre que

$$1 + 2\cos\theta + 2\cos(2\theta) + \cdots + 2\cos((n-1)\theta) = \frac{\mathrm{sen}\left(\left(n-\frac{1}{2}\right)\theta\right)}{\mathrm{sen}\left(\frac{\theta}{2}\right)}$$

y

$$\mathrm{sen}\theta + \mathrm{sen}(2\theta) + \cdots + \mathrm{sen}((n-1)\theta) = \frac{\cos\left(\frac{\theta}{2}\right) - \cos\left(\left(n-\frac{1}{2}\right)\theta\right)}{2\ \mathrm{sen}\left(\frac{\theta}{2}\right)}.$$

14. Pruebe que no existe un número complejo z tal que $|z| - z = i$

15. Encuentre $z \in \mathbb{C}$ tal que

 a) $\bar{z} = i(z-1)$
 b) $z^2\bar{z} = z$
 c) $|z+3i| = 3|z|$

16. Sea $z = \cos\theta + i\mathrm{sen}\theta$, muestre que $z^m + z^{-m} = 2\cos(m\theta)$, para todo m entero.

17. Encuentre números reales x e y satisfaciendo cada una de las siguientes ecuaciones

 a) $\frac{x}{1+2i} + \frac{y}{3+2i} = \frac{5+6i}{8i-1}$
 b) $x - yi = \frac{1}{2-5i}$
 c) $x + yi = (1-i)^4$

18. Sean a, b, c números reales con $a \neq 0$ y $b \neq c$. Si $\frac{1}{z-ci} = \frac{1}{a+bi} + \frac{1}{a+ci}$, encuentre $|z|^2$.

19. Suponga que $|z + ai| = |z + bi|$ donde a y b son números reales distintos. Muestre que $z - \bar{z} = -(a + b)i$.

20. Suponga que $4|z + 1| = |z + 16|$, muestre que $|z| = 4$.

21. Dé una descripción geométrica de los siguientes conjuntos

 a) $A = \{z : |z - 1| = |z - i|\}$
 b) $A = \{z : (1 + i)z + (1 - i)\bar{z} = 1\}$
 c) $A = \{z : z\bar{z} + iz - i\bar{z} - 3 = 0\}$

22. Muestre que si $z \neq -1$ y $|z| = 1$, entonces $2\text{Arg}(1 + z) = \text{Arg}(z)$.

23. Suponga que $\text{Re}z > 0$, muestre que $|z + \sqrt{z^2 - 1}| \geq 1$, y la igualdad sólo se presenta si z es un real en $(0, 1]$.

24. Muestre que en general no es cierto, para números complejos z y w, que $\sqrt{zw} = \sqrt{z}\sqrt{w}$.

25. Sean z y w números complejos diferentes de cero, muestre que
$$|z + w| \geq \frac{1}{2}(|z| + |w|)\left|\frac{z}{|z|} + \frac{w}{|w|}\right|.$$

26. ¿Para qué números complejos z es cierto que $\sqrt{\frac{z}{\bar{z}}} = \frac{z}{|z|}$?

27. Muestre que el sistema de matrices de la forma especial
$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix},$$
combinado con la suma y multiplicación de matrices usuales, es isomorfo al campo de los complejos.

28. Pruebe que
$$\left|\frac{a - b}{1 - \bar{a}b}\right| = 1,$$
si $|a| = 1$ o $|b| = 1$. ¿Qué excepción debe ser hecha si $|a| = |b| = 1$?

29. Pruebe que
$$\left|\frac{a - b}{1 - \bar{a}b}\right| < 1,$$
si $|a| < 1$ y $|b| < 1$.

30. Muestre que existen números complejos z satisfaciendo
$$|z - a| + |z + a| = 2|c|$$
si y sólo si $|a| \leq |c|$.

31. Si $|a_i| < 1$, $\lambda_i \geq 0$ y $\lambda_1 + \lambda_2 + \cdots + \lambda_n = 1$, para $i = 1, 2, ..., n$. Muestre que
$$|\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n| < 1.$$

Capítulo 10

Polinomios

Todas las personas que han pasado por la secundaria sabe lo que es un polinomio con sólo verlo. En términos generales un polinomio es una expresíon matemática la cual tiene un conjunto finito de variables y contastes relacionadas con las operaciones básicas de suma, resta, multiplicación y las variables tienen como exponentes enteros positivos. El estudio de los polinomios se remonta a los antiguos Egipcios y Babilonios quienes eran capaces de resolver ecuaciones de la forma $ax = b$, $ax^2 + bx = c$ y $x^2 + y^2 = z^2$, y el método inventado por ellos es casi el mismo que se usa en la actualidad. Es claro que el desarrollo subsecuente que tuvo la teoría de polinomios dío origen a lo que en la actualidad llamamos Álgebra y las hermosas conecciones que existen con la geometría, como lo son la Geometría Analítica y Algebraica. Los polinomios son de mucha utilidad en áreas como Análisis Numérico, Ecuaciones Diferenciales Ordinarias, Mecánica Cuantica, Espacios de Hilbert y otras donde usualmente son utillizados para aproximar todo tipo de funciones, los más conocidos son los polinomios de Hermite, Legendre, Laguerre y Chebyshov. En este capítulo estudiaremos polinomios sobre los númeroa reales y complejos, nos centraremos en la existencia de raíces, factorización y división sintética.

10.1. Definiciones Básicas

Sean $\langle F_1; +, \cdot \rangle$ y $\langle F_2; +, \cdot \rangle$ dos campos, con $F_2 \subseteq F_1$, x una variable cuyo universo es F_1, n un entero positivo y las constantes $a_0, a_1, \cdots, a_n$ son elementos de F_2.

Definición 10.1 (Polinomio)**.** *Un polinomio en $x \in F_1$ sobre el campo F_2, se denota por $P(x)$ y está definido por*

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0. \tag{10.1}$$

En el polinomio P(x), a_i es el coeficiente de $x^i, i = 0, 1, 2, \cdots, n, a_n$ es el coeficiente principal y a_0 es el coeficiente final o término constante.

Si $F_1 = F_2 = \mathbb{C}$, llamamos a $P(x)$ un polinomio complejo. Si $F_1 = F_2 = \mathbb{R}$, llamamos a $P(x)$ un

polinomio real. Los siguientes son ejemplos de polinomios

$$P(x) = (2+i)x^4 - \sqrt{3}x + 4, \quad Q(x) = x^2 - \sqrt{2}x - 5, \quad R(x) = 5.$$

Definición 10.2 (Grado de un polinomio)**.** *Si en el polinomio $P(x)$, dado en (10.1), se tiene que $a_n \neq 0$, entonces $P(x)$ es un polinomio de grado n en x.*

En el ejemplo anterior $P(x)$ es un polinomio de grado 4, $Q(x)$ es un polinomio de grado 2 y $R(x)$ es un polinomio de grado cero.

Definición 10.3. *Si todos los coeficientes en el polinomio $P(x)$ dado en (10.1) son cero, decimos que $P(x)$ es el polinomio nulo. Seguimos la convención de no asignar grado al polinomio nulo. Si $n = 0$ y $a_0 \neq 0$, entonces $P(x) = a_0$ se llama polinomio constante. Un polinomio de grado $n \geq 1$ es un polinomio no constante.*

Definición 10.4 (Ecuación polinomial)**.** *Si $P(x)$ es un polinomio de grado n en $x \in F_1$ sobre F_2, llamamos a la ecuación $P(x) = 0$, ecuación polinomial de grado n en $x \in F_1$ sobre F_2. Más exactamente,*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0. \tag{10.2}$$

El conjunto solución de la ecuación (10.2) se denota por

$$\{x \in F_1 : a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0\}$$

Definición 10.5. *Si $P(x)$ es un polinomio de grado n en $x \in F_1$ sobre F_2, entonces la función*

$$P = \{(x, y) : y = P(x)\}$$

es llamada función polinomial de grado n y

$$Dom\ P = F_1 \qquad y \qquad Ran\ P \subseteq F_1$$

Una función polinomial es una función polinomial de grado n o la función cero $\{(x, y) : y = 0\}$

10.2. Ecuaciones Polinomiales de Segundo Grado

Cualquier ecuación polinomial de segundo grado, puede escribirse en la forma

$$ax^2 + bx + c = 0$$

donde $a, b, c \in F_2, a \neq 0$ y $x \in F_1$, siendo $F_2 \subseteq F_1$. Una ecuación polinomial de segundo grado, se llama frecuentemente ecuación cuadrática.

Las pruebas de los siguientes teoremas son muy sencillas, por tal motivo no las haremos.

Teorema 10.6. *Sean $a, b, c \in \mathbb{R}$ con $a \neq 0$ y considere $x \in \mathbb{R}$.*

(i) *Si* $b^2-4ac>0$, *entonces*
$\{x : ax^2+bx+c=0\} = \left\{\frac{-b+\sqrt{b^2-4ac}}{2a},\ \frac{-b-\sqrt{b^2-4ac}}{2a}\right\}.$

(ii) *Si* $b^2-4ac=0$, *entonces*
$\{x : ax^2+bx+c=0\} = \left\{\frac{-b}{2a}\right\}.$

(iii) *Si* $b^2-4ac<0$, *entonces*
$\{x : ax^2+bx+c=0\} = \varnothing.$

Definición 10.7 (Raíz de un polinomio). *Un elemento del conjunto solución de una ecuación polinomial* $P(x)=0$, *se llama raíz del polinomio* $P(x)$*; es decir, una raíz de un polinomio* $P(x)$ *es un número* r *con la propiedad que* $P(r)=0$.

Teorema 10.8. *Sean* $a,b,c \in \mathbb{R}$ *con* $a \neq 0$ *y considere* $x \in \mathbb{C}$. *Entonces se tienen los mismos resultados* (i) *y* (ii) *excepto que* (iii) *cambia por:*

$(iii)'$ *Si* $b^2-4ac<0$, *entonces*
$$\{x : ax^2+bx+c=0\} = \left\{\frac{-b+i\sqrt{-(b^2-4ac)}}{2a}, \frac{-b-i\sqrt{-(b^2-4ac)}}{2a}\right\}$$

10.3. Factorización de Polinomios

A continuación enunciamos uno de los teoremas más importantes de este capítulo, para lo cual necesitamos la siguiente definición. Cualquier polinomio $P(x)$ en $x \in \mathbb{C}$ sobre $\mathbb{C}$ será llamado un polinomio complejo.

Teorema 10.9 (Teorema Fundamental del Álgebra). *Cualquier polinomio complejo de grado* $n \geq 1$, *tiene al menos una raíz.*

La demostración de este importante teorema usa elementos de variable compleja (Teorema de Liouville) lo cual se sale de los objetivos del libro, por tal motivo lo aceptaremos como cierto y lo usaremos para deducir otras propiedades de los polinomios. La prueba del Teorema Fundamental del Ágebra nos garantiza la existencia de por lo menos una raíz, pero no nos dice cuál es la raíz ni cómo hallarla.

El siguiente teorema es enunciado sin demostración, la cual es un poco tediosa y será omitida para efectos de rapidez.

Teorema 10.10. Algoritmo de la División: *Sean* $P(x)$ *un polinomio de grado* $n \geq 1$ *en* $x \in F_1$ *sobre* F_2 *y* $D(x)$ *un polinomio de grado* m *en* $x \in F_1$ *sobre* F_2, *con* $0 \leq m \leq n$. *Entonces existen polinomios únicos* $Q(x)$ *y* $R(x)$ *en* $x \in F_1$ *sobre* F_2, *que tienen la propiedad de que*

$$P(x) = D(x) \cdot Q(x) + R(x),$$

y si $R(x)$ *tiene un grado (no es el polinomio nulo), entonces este grado es menor que el grado de* $D(x)$.

Definición 10.11. *Si $P(x), D(x)$ y $Q(x)$ son polinomios en en $x \in F_1$ sobre el campo F_2 y si*

$$P(x) = D(x) \cdot Q(x) \tag{10.3}$$

Entonces (10.3) se llama una factorización de $P(x)$ sobre F_2 y $D(x)$, $Q(x)$ se llaman factores (polinomiales) de $P(x)$ sobre F_2.

Note que cuando $D(x)$ es un polinomio de grado $m \geq 1$, entonces $D(x)$ es un factor de $P(x)$ únicamente si el residuo $R(x)$, dado por el algoritmo de la división, es el polinomio cero.

Teorema 10.12 (Teorema del Residuo)**.** *Si un polinomio $P(x)$ en $x \in F_1$ sobre $F_2 \subseteq \mathbb{C}$ es dividido por $x - r$, donde $r \in F_2$, para obtener un cociente $Q(x)$ y un residuo R, entonces $P(r) = R$.*

Prueba: Por el algoritmo de la división $P(x) = (x - r)Q(x) + R(x)$, con grado de R menor que 1. Si $R(x) = 0$, concluimos que $P(x) = (x - r)Q(x)$, lo cual trivialmente nos da que $P(r) = 0 = R$. Suponga que $R(x)$ no es cero, entonces como el grado de un polinomio es un número entero se tiene que el grado de $R(x)$ es cero, así que $R(x) = R$, donde R es una constante. Luego

$$P(x) = (x - r)Q(x) + R$$

Lo que implica que $P(r) = 0 + R = R$. □

Una consecuencia bien interesante del teorema anterior es lo siguiente

Teorema 10.13 (Teorema del Factor)**.** *Sean $P(x)$ un polinomio en $x \in F_1$ sobre $F_2 \subseteq \mathbb{C}$ y $r \in F_2$. Entonces r es una raíz de $P(x)$ si y sólo si $x - r$ es un factor de $P(x)$*

Prueba: "⇒"Por el algoritmo de la división tenemos que $P(x) = (x - r)Q(x) + R(x)$. El teorema anteriosr nos dice que $0 = P(r) = R$. Así que $P(x) = (x - r)Q(x)$, lo que indica que $(x - r)$ es un factor t=de $P(x)$.
"⇐"Fácil y es dejada como ejercicio al lector. □

Definición 10.14. *En (10.3) el polinomio $D(x)$ lo llamaremos un factor propio de $P(x)$ si su grado es menor que el grado de $P(x)$, pero no cero; $D(x)$ es llamado un factor impropio de $P(x)$ si el grado de $D(x)$ es igual al grado de $P(x)$ o es cero.*

Definición 10.15. *Un polinomio $P(x)$ de grado $n \geq 1$ en $x \in F_1$ sobre F_2 es irreducible sobre F_2 si $P(x)$ no tienen factores propios cuyos coeficientes están en F_2. Diremos que $P(x)$ es reducible sobre F_2 si $P(x)$ tiene factores propios cuyos coeficientes están en F_2.*

Ejemplo 10.16. *$x^2 - 5$ es irreducible sobre $\mathbb{Q}$, pero es reducible sobre $\mathbb{R}$.*

Con este lenguaje podemos re-escribir los siguientes teoremas.

Teorema 10.17. *El polinomio real $P(x) = ax^2+bx+c$ es inreducible sobre $\mathbb{R}$ si y sólo si $b^2-4ac < 0$.*

Teorema 10.18. *El polinomio Complejo $P(x) = ax^2 + bx + c$ es siempre reducible sobre el campo $\mathbb{C}$.*

Un resultado importante e interesante, el cual no demostraremos es el siguiente.

Teorema 10.19. *Cualquier polinomio reducible sobre F_2 puede escribirse como un producto de la forma*

$$P(x) = a_n P_1(x) P_2(x) \cdots P_k(x) \tag{10.4}$$

donde a_n es el coeficiente principal de $P(x)$ y $P_1(x)$, $P_2(x)$, $\cdots P_k(x)$ son polinomios irreducibles sobre F_2 y cada uno tiene como coeficiente principal 1. Además una factorización de tal tipo es única excepto por el orden de los factores.

Ejemplo 10.20. *Como ilustración del resultado anterior considere $3x^4 - 75$ sobre $\mathbb{Q}$. En este caso se tiene que*

$$3x^4 - 75 = 3(x^2 - 5)(x^2 + 5),$$

donde x^2-5 y x^2+5 son polinomios irreducibles sobre $\mathbb{Q}$. Si consideramos $3x^4-75$ sobre $\mathbb{R}$, tenemos que

$$3x^4 - 75 = 3(x - \sqrt{5})(x + \sqrt{5})(x^2 + 5),$$

donde $(x-\sqrt{5})$, $(x+\sqrt{5})$ y (x^2+5) son polinomios irreducibles sobre $\mathbb{R}$. Finalmente, si consideramos $3x^4 - 75$ como un polinomio sobre $\mathbb{C}$, se obtiene

$$3x^4 - 75 = 3(x - \sqrt{5})(x + \sqrt{5})(x + i\sqrt{5})(x - i\sqrt{5}).$$

Definición 10.21. *Cuando un polinomio $P(x)$ en $x \in F_1$ sobre F_2 es escrito como el producto de la forma (10.4) decimos que $P(x)$ está completamente factorizado sobre F_2.*

Teorema 10.22. *Un polinomio complejo $P(x)$ de grado $n \geq 1$,*

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

puede ser expresado como el producto del número complejo a_n y n factores de primer grado y de la forma $(x - r_i)$, donde $r_i \in \mathbb{C}$ $(i = 1, 2, \cdots, n)$. Es decir, la factorización completa de $P(x)$ es

$$P(x) = a_n(x - r_1)(x - r_2) \cdots (x - r_{n-1})(x - r_n).$$

Prueba: Por el Teorema Fundamental del Álgebra $P(x)$ tiene al menos una raíz que podemos denotar r_1. Entonces por el Teorema del Factor $(x - r_1)$ es un factor de $P(x)$, luego

$$P(x) = (x - r_1)P_1(x)$$

donde $P_1(x)$ es un polinomio complejo de grado $n-1$ y con a_n como coeficiente principal. Si $n = 1$, entonces $P_1(x) = a_1$ y termina la prueba. Si $n \geq 2$, entonces $P_1(x)$ es un polinomio complejo de grado $m \geq 1$, luego $P_1(x)$ tiene al menos una raíz que podemos denotar r_2 entonces

$$P(x) = (x - r_1)(x - r_2)P_2(x).$$

donde $P_2(x)$ es un polinomio complejo de grado $n-2$ y con a_n como coeficiente principal. Si $n=2$, entonces $P_2(x)=a_2$ y termina la prueba. Este mismo procedimiento puede ser usado en total n veces para mostrar la existencia de $r_1, r_2, \cdots, r_n \in \mathbb{C}$ tales que

$$P(x) = (x-r_1)(x-r_2)\cdots(x-r_n)P_n(x),$$

con $P_n(x)$ un polinomio de grado cero y coeficiente principal a_n, es decir $P_n(x)=a_n$, lo que termina la prueba. □

Teorema 10.23. *Un polinomio complejo de grado $n \geq 1$ tiene a lo sumo n raíces. Un polinomio de grado cero no tiene raíces.*

Definición 10.24. *El número de veces que un factor $x-s_i$ aparece en la factorización completa de un polinomio complejo se llama la multiplicidad de la raíz s_i.*

Teorema 10.25. *El conjunto solución $\{x \in \mathbb{C} : P(x)=0\}$ de una ecuación polinomial compleja de grado n, tiene k elementos $s_1, s_2, \cdots, s_k$, donde $k \leq n$. Los números s_i son las raíces del polinomio $P(x)$ y si m_i es la multiplicidad de la raíz s_i, entonces $m_1+m_2+\cdots+m_k=n$.*

Prueba: Es claro que podemos escribir $P(x)$ de la siguiente forma

$$P(x) = a_n(x-s_1)^{m_1}(x-s_2)^{m_2}\cdots(x-s_k)^{m_k},$$

donde $s_i \neq s_j$, para $i \neq j$ y $1 \leq i,j \leq k$. Así que los s_i son las raíces distintas de $P(x)$ y por el Teorema 10.23 se tiene que $k \leq n$. Además, como

$$a_n(x-s_1)^{m_1}(x-s_2)^{m_2}\cdots(x-s_k)^{m_k}$$

es de grado n, tenemos que $m_1+m_2+\cdots+m_k=n$. □

El siguiente resultado es bien interesante, nos dice que si dos polinomios de grado n coinciden en $n+1$ puntos distintos, entonces son iguales.

Teorema 10.26. *Sean $P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ y $Q(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$ polinomios complejos de grado n. Si existen $n+1$ números distintos $x_1, x_2, \cdots, x_n, x_{n+1}$ con la propiedad que*

$$P(x_i)=Q(x_i) \quad \text{para cada} \quad i=1,2,\cdots,n+1.$$

Entonces $a_k=b_k$, para $k=0,1,\cdots,n$ y $P(x)-Q(x)$ es el polinomio nulo.

Prueba: Definamos $R(x)=P(x)-Q(x)$ y supongamos que $R(x)$ tiene grado m. Entonces $0 \leq m \leq n$ por ser la diferencia de polinomios de grado n. Si $m=0$, entonces $R(x)$ es un polinomio constante y como $R(x_1)=0$, se tiene que $R(x)$ es el polinomio nulo. Supongamos que $m \geq 1$, entonces por el Teorema 10.23 $R(x)$ tiene a lo sumo n raíces. Pero $R(x_i)=0$ para $i=0,1,2,\cdots,n+1$. Luego $R(x)$ tiene $n+1$ raíces distintas, lo cual es absurdo. Por tanto $R(x)$ no debe tener grado, lo que implica $R(x)=0$. □

10.4. Polinomios Sobre $\mathbb{R}$

En esta sección estudiaremos polinomios en $x \in \mathbb{C}$ sobre $\mathbb{R}$. Los llamaremos polinomios sobre $\mathbb{R}$. Note que el conjunto de los polinomios en $x \in \mathbb{C}$ sobre $\mathbb{R}$ es un subconjunto de los polinomios en $x \in \mathbb{C}$ sobre $\mathbb{C}$. Por consiguiente por el Teorema Fundamental del Álgebra, cada polinomio de grado $n \geq 1$ sobre $\mathbb{R}$ tiene por lo menos una raíz.

Teorema 10.27. *Si un polinomio $P(x)$ sobre $\mathbb{R}$ tiene una raíz compleja z y $\mathrm{Im} z \neq 0$, entonces $\overline{z}$ es también raíz de $P(x)$.*

Prueba: Como z es raíz de $P(x)$, entonces por el Teorema del Factor $x - z$ es un factor de $P(x)$. Probaremos que $x - \overline{z}$ es un factor de $P(x)$, lo que terminaría la prueba. Sea $z = a + b_i$. Consideremos

$$D(x) := (x - \overline{z})(x - z) = (x - a)^2 + b^2$$

y dividamos $P(x)$ por $D(x)$. Por el Algoritmo de la División se tiene que

$$P(x) = D(x)Q(x) + R(x),$$

donde el grado de $R(x)$ es estrictamente menor que 2. Si $R(x) = 0$ termina la prueba. Supongamos que $R(x)$ no es el polinomio cero, entonces como $P(x)$ y $D(x)$ son polinomios sobre $\mathbb{R}$, existen $r, t \in \mathbb{R}$ tales que $R(x) = rx + t$. Luego

$$P(x) = D(x)Q(x) + rx + t.$$

Note que $0 = P(z) = rz + t$, entonces $(ra + t) + irb = 0$. Lo que implica que $ra + t = 0$ y $rb = 0$. Como $b \neq 0$ se tiene que $r = 0$ y $t = 0$. Consecuentemente

$$P(x) = (x - z)(x - \overline{z})Q(x),$$

lo que termina la prueba. □

Como resultado inmediato del teorema anterior tenemos que las raíces no reales de un polinomio vienen en pares conjugados. Mas exactamente,

Corolario 10.28. *Si un polinomio $P(x)$ en $x \in \mathbb{C}$ sobre $\mathbb{R}$ tiene algunas raíces que no son reales, entonces tiene un número par de raíces que no son números reales.*

Teorema 10.29. *Un polinomio de grado impar sobre $\mathbb{R}$ tiene al menos una raíz que un número real.*

Prueba: Por el Teorema 10.22 cualquier polinomio $P(x)$ de grado $n \geq 1$ puede escribirse como

$$P(x) = a_n(x - r_1)(x - r_2) \cdots (x - r_n),$$

donde $r_i \in \mathbb{C}$. Por el teorema anterior si cualquiera de los números r_i no es real, entonces existe un número par de $r_i's$ que no son reales. Como n es un número impar, debe existir por lo menos un r_i que es real, lo que termina la prueba. □

Teorema 10.30. *Un polinomio $P(x)$ de grado $n \geq 1$ en $x \in \mathbb{C}$ sobre $\mathbb{R}$ puede escribirse como un producto de polinomios sobre $\mathbb{R}$ que son irreducibles sobre $\mathbb{R}$ y que son de grado uno o dos.*

Prueba: Sabemos que $P(x) = a_n(x - r_1)(x - r_2)\cdots(x - r_n)$. Si uno de los r_i es un complejo con $\text{Im}r_i \neq 0$ por el Teorema 10.27 existe r_j con $i \neq j$ tal que $r_j = \overline{r_i}$. Así que si $r_i = a_i + ib_i$, tenemos que $D(x) = x^2 - 2a_ix + a_i^2 + b_i^2$ debe ser un factor de $P(x)$. Note que $D(x)$ es de grado dos e irreducible sobre $\mathbb{R}$. Repitiendo este argumento para todos los $r_i's$ que tengan $\text{Im}r_i \neq 0$ terminamos la prueba del teorema. □

Si un polinomio de grado $n \geq 1$ sobre $\mathbb{R}$ tiene alguna raíz racional, el siguiente teorema ayuda a determinarla.

Teorema 10.31. *Sea*

$$P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

Un polinomio cuyos coeficientes son enteros si p/q es un número racional que es una raíz de $P(x)$, entonces p es un factor entero de a_0 y q es un factor entero de a_n.

Prueba: Como $P\left(p/q\right) = 0$, entonces

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0. \tag{10.5}$$

Multiplicando por q^n se tiene que

$$a_np^n + a_{n-1}p^{n-1}q + \cdots + a_1pq^n = -a_0q^n.$$

Si $p = 0$, entonces $a_0 = 0$ y la primera parte del teorema estaría probada. Supongamos que $p \neq 0$, multiplicando la igualdad anterior por $1/p$ obtenemos

$$a_np^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1q^n = \frac{-a_0q^n}{p}$$

Como a_i, con $i = 1, 2, \cdots n$ y p son enteros, y $q \in \mathbb{N}$, se tiene que $\frac{-a_0q^n}{p}$ es un entero. Lo que indica que p divide a a_0q^n. Como p y q son primos relativos, se sigue que p y q^n también son primos relativos, consecuentemente p divide a a_0. Lo que muestra la primera parte del teorema.

Ahora, multiplique (10.5) por q^{n-1} para obtener

$$a_{n-1}p^{n-1} + a_{n-2}p^{n-2}q + \cdots + a_1pq^{n-2} + a_0q^{n-1} = \frac{-a_np^n}{q}.$$

Por un argumento similar al hecho anteriomente concluimos que q es un factor entero de a_n, lo cual termina la prueba. □

10.5. División Sintética

Supóngase que

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{10.6}$$

es el dividendo en el polinomio de división; es decir, asuma que $P(x)$ es un polinomio de grado n en $x \in F_1$ sobre F_2, donde $F_2 \subseteq F_1$. Además, supóngase que el divisor en el algoritmo de división es un polinomio $x - r$ de grado uno con $r \in F_2$. Entonces, por el algoritmo de división

$$P(x) = (x - r) \cdot Q(x) + R \tag{10.7}$$

donde $Q(x)$ es un polinomio de grado $n-1$ en $x \in F_1$ sobre F_2 y R es un elemento de F_2. Escribimos

$$Q(x) = b_n x^{n-1} + b_{n-1}x^{n-2} + \cdots + b_2 x + b_1 \tag{10.8}$$

y deseamos determinar R y los coeficientes de $Q(x)$ en términos de los coeficientes de $P(x)$. Usando las notaciones (10.6) y (10.8) podemos escribir (10.7) como

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - r)(b_n x^{n-1} + b_{n-1}x^{n-2} + \cdots + b_2 x + b_1) + R$$

o como

$$\begin{aligned} a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = b_n x^n + (b_{n-1} - rb_n)x^{n-1} + (b_{n-2} - rb_{n-1})x^{n-2} + \cdots \\ + (b_1 + rb_2)x + (R - rb_1) \end{aligned} \tag{10.9}$$

ahora(10.7), y por consiguiente (10.9), se cumplen para toda $x \in F_1$ y por lo tanto, (suponiendo que hay más de n números en el campo F_1) la igualdad (10.9) se cumple para $n + 1$ valores de x por lo menos. Entonces. por el Teorema 10.26, los coeficientes correspondientes de los polinomios (10.9) son iguales; es decir,

$$a_n = b_n,\ a_{n-1} = b_{n-1} - rb_n, \cdots, a_1 = b_1 - rb_2,\ a_0 = R - rb_1.$$

Estas igualdades pueden escribirse en la forma

$$b_n = a_n,\ b_{n-1} = a_{n-1} + rb_n, \cdots, b_1 = a_1 - rb_2,\ R = a_0 + rb_1. \tag{10.10}$$

Obsérvese que las igualdades (10.10) nos permiten expresar los coeficientes sucesivos de $Q(x)$ y R en términos de los coeficientes de $P(x)$ y $Q(x)$ los cuales están dados. Para propósitos de cálculo, es conveniente ordenar este trabajo en la forma tabular mostrada a continuación, donde por (10.10), la suma de cualquier par de componentes en la primera y segunda líneas columna vertical dada es el componente en la tercera línea de la misma columna.

a_n	a_{n-1}	a_{n-2}	$\cdots$	a_1	a_0
	rb_n	rb_{n-1}	$\cdots$	rb_2	rb_1
b_n	b_{n-1}	b_{n-2}	$\cdots$	b_1	R

De la última línea de esta tabla escribimos el cociente

$$Q(x) = b_n x^{n-1} + b_{n-1}x^{n-2} + \cdots + b_1$$

y el residuo

$$R = a_0 + rb_1.$$

Definición 10.32. *El procedimiento que hemos dado anteriormente para determinar el cociente $Q(x)$ y el residuo R en la división de $P(x)$ por $x-r$ se llama división sintética.*

A continuación mostramos una forma práctica de aplicar el algoritmo dado arriba. Si queremos dividir $P(x)$ por $x-r$ usando la división sintética, primero ordenamos $P(x)$ en potencias decrecientes de x, completando todos los términos faltantes con ceros como coeficientes y entonces, escribimos los coeficientes $a_n, a_{n-1}, a_{n-2}, \cdots, a_1, a_0$ en una línea horizontal. Bajamos el coeficiente principal $a_n(= b_n)$ a la posición de una tercera línea horizontal. Multiplicamos a_n por r y colocamos el producto sobre la segunda ínea horizontal bajo el segundo coeficiente a_{n-1}. Sumamos a_{n-1}, y el producto $a_n r$, colocando dicha suma (b_{n-1}) en la tercera línea. Multiplicamos b_{n-1} por r y colocamos el producto en la segunda línea debajo de a_{n-2}. Sumamos a_{n-2} y el producto $b_{n-1}r$, colocando dicha suma (b_{n-2}) en la tercera línea. Continuamos de esta manera hasta que el producto de b_1 y r esté colocado en la segunda línea debajo de a_0. Cuando a_0 y el producto rb_1 se suman, el resultado es el residuo R; éste se coloca en la tercera línea y el proceso se detiene.

Ejemplo 10.33. *Determinar el cociente $Q(x)$ y el residuo R cuando $P(x) = x^4 + 2x^3 - 6x + 1$ es dividido por $x - 2$.*

En este caso $P(x) = x^4 + 2x^3 + 0x^2 - 6x + 1$ y ordenamos el trabajo como sigue

1	2	0	−6	1	2
	2	8	16	20	
1	4	8	10	21	

por lo tanto, el cociente es

$$Q(x) = x^3 + 4x^2 + 8x + 10$$

y el residuo es $R = 21$.

Por el Teorema del residuo, si $P(x)$ es dividido por $x - r$, el residuo R es igual a $P(r)$. Por consiguiente, la división sintética puede usarse ventajosamente para calcular $P(r)$, como ilustración en el ejercicio anterior tenemos que $P(2) = 21$.

10.6. Ejercicios

1. Factorizar $x^4 - 5x^2 - 36$ completamente sobre $\mathbb{Q}$, $\mathbb{R}$, y $\mathbb{C}$.
2. Dividir $x^4 - 14x^3 + 2x^2 + 49x - 36$ por $x + 2$, identificar el cociente y el residuo en esta división.
3. Usando el Teorema del Factor, mostrar que el primer polinomio es un factor del segundo.
 a) $x - 1$; $4x^3 + 3x^2 - 5x - 2$
 b) $x - 2$; $2x^3 - 11x^2 + 17x - 6$
4. Factorizar los siguientes polinomios completamente sobre $\mathbb{C}$

a) $P(x) = x^3 - 5x^2 - 17x + 21$. Una raíz de $P(x)$ es 7.

b) $Q(x) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$. Una raíz de $Q(x)$ es 1 con multiplicidad dos.

5. Determinar un polinomio complejo $P(x)$ de grado tres que tenga como raíces $1+\sqrt{3}$ y $1-\sqrt{3}$, esta última de multiplicidad dos.

6. Determinar un polinomio $Q(x)$ de grado cuatro en $x \in \mathbb{C}$ sobre $\mathbb{R}$, que tenga como raíz $1+i$ de multiplicidad dos

7. Mostrar que:

a) $x - a$; es factor de $x^n - a^n$, para cada $n \in \mathbb{N}$.

b) $x + a$; es factor de $x^n - a^n$, para cada $n \in \mathbb{N}$ par.

c) $x + a$; no es factor de $x^n - a^n$, si $n \in \mathbb{N}$ es impar.

d) $x + a$; es factor de $x^n + a^n$, para cada $n \in \mathbb{N}$ impar.

8. Mostrar que si un polinomio de tercer grado en $x \in \mathbb{C}$ sobre $\mathbb{R}$ tiene una raíz no real, entonces tiene únicamente una raíz real y un factor de segundo grado irreducible sobre $\mathbb{R}$.

9. Usar la división sintética para determinar el cociente $Q(x)$ y el residuo R en la división del primer polinomio por el segundo.

a) $x^4 - 14x^3 + 2x^2 + 49x - 36; \quad x + 2$

b) $3x^3 - \frac{1}{5}x^2 + \frac{3}{10}x - \frac{23}{1000}; \quad x - \frac{3}{10}$.

c) $x^3 - (6+i)x^2 + (11+5i)x - (6+6i); \quad x - (1-i)$

10. Determine las raíces racionales de los siguientes polinomios

a) $2x^3 - x^2 + 5$

b) $20x^3 + 11x^2 - 8x + 1$

c) $x^4 - x^3 - 4x^2 - x + 1$

11. Muestre que si $P(x)$ es un polinomio sobre $\mathbb{Q}$ y $a+\sqrt{b}$ es una raíz de $P(x)$ con $a \in \mathbb{Q}$ y $\sqrt{b} \in \mathbb{I}$, entonces $a - \sqrt{b}$ es también raíz e $P(x)$.

12. ¿Para qué valores de k puede $P(x) = (k+2)x^2 + 6kx + 7k + 5$ tener una raíz de multiplicidad dos?

13. Demostrar que para $a, b, c \in \mathbb{R}$ las únicas raíces del polinomio

$$P(x) = 2(a+b)x^2 - 2(a+b+c)x + c$$

son números reales.

14. Demostrar que para $a \in \mathbb{Q}$ las únicas raíces del polinomio

$$P(x) = 5ax^2 - (5a+3)x + 3$$

son números racionales.

15. Si r_1, r_2 y r_3 son las raíces del polinomio $P(x) = x^3+ax^2+bx+c$, mostrar que $r_1+r_2+r_3 = -a$, $r_1r_2 + r_1r_3 + r_2r_3 = b$ y $r_1r_2r_3 = -c$.

16. Muestre que el único polinomio $P(x)$ de grado $n-1$ que tiene raíces $x_2, x_3, \cdots, x_n$ y tal que $P(x_1) = 1$ es
$$P(x) = \frac{Q(x)}{(x-x_1)Q'(x_1)},$$
donde $Q(x) = (x-x_1)(x-x_2)\cdots(x-x_n)$.

17. Sean $x_1, x_2, \cdots, x_n \in C$ distintos entre si, $y_1, y_2, \cdots y_n \in \mathbb{C}$ y $Q(x) = (x-x_1)(x-x_2)\cdots(x-x_n)$. Muestre que
$$P(x) = \sum_{i=1}^{n} \frac{Q(x)}{(x-x_i)Q'(x_i)},$$
tiene grado no mayor que $n-1$, $P(x_i) = y_i$ para cada $i = 1, 2, \cdots n$ y $P(x)$ es único con las propiedades anteriores.

18. Sea $P(x)$ un polinomio en $\mathbb{C}$ de grado n. Suponga que $a_1, a_2, \cdots, a_n$ son las raíces de $P(x)$. Si b es una raíz de $P'(x)$, muestre que existen números complejos $\lambda_1, \lambda_2, \cdots, \lambda_n$ tales que
$$\sum_{k=1}^{n} \lambda_k = 1 \quad \text{y} \quad b = \sum_{k=1}^{n} a_k\lambda_k.$$
Sugerencia: Considere el cociente $P'(x)/P(x)$.

19. Sean $p, q \in \mathbb{R}$. Muestre que $4p^3 + 27q^2 = 0$ es una condición necesaria y suficiente para que el polinomio $P(x) = x^3 + px + q$ tenga una raíz doble.

20. Pruebe que $P(x) = 30x^n - 91$ no tiene raíces racionales para cada $n \geq 2$.

21. Encuentre $a \in \mathbb{R}$ tal que $z = -i$ sea una raíz del polinomio $P(z) = z^3 - z^2 + z + 1 + a$. Además, para tal valor de a encuentre los factores de $P(z)$ en $\mathbb{R}$ y en $\mathbb{C}$.

22. Decimos que un polinomio $P(x)$ divide a un polinomio $Q(x)$, lo cual denotamos como $P|Q$, si existe un polinomio $C(x)$ tal que $Q(x) = C(x)P(x)$. Muestre que si $P(x)$ divide a $Q(x)$ y $Q(x)$ divide a $P(x)$, existe una constante c tal que $Q(x) = cP(x)$.

23. Suponga que $P(x)$ es un polinomio de grado $n \geq 1$ tal que $P(k) = \frac{k}{k+1}$, para $k = 0, 1, ..., n$. Encuentre $P(n+1)$.

24. Sean r, s, t raíces del polinomio complejo $x^3 + ax^2 + bx + c$. Encuentre, en términos de a, b y c, un polinomio cúbico cuyas raíces sean $rs + t, st + r, tr + s$.

25. Encuentre de forma explícita tres números complejos x, y, z tales que $x+y+z = xy+xz+yz = 3$ y $xyz = 9$.

26. Sea $P(x)$ un polinomio real de grado n, y suponga que las constantes $c_0, c_1, ..., c_n$ satisfacen $c_0P(x) + c_1P(2x) + c_2P(2^2x)\cdots + c_nP(2^nx) = 0$. Muestre que $c_i = 0$ para todo $i = 0, 1, ..., n$.

Bibliografía

[1] Bloch, Ethan, *Proof and Fundamentals,* Birkhäuser, Boston, 2000.

[2] Burn, R., *Numbers and functions*, Second Edition, Cambridge University Press, 2004.

[3] Devlin, Keith, *Sets, functions, and logic*, Third Edition, Chapman & Hall, 2005.

[4] Gerstein, Larry, *Introduction to Mathematical structures and proofs*, Springer, New York, 1996.

[5] Maddox, Randall, *A transition to abstract mathematics*, Second Edition, Elsevier Academic Press, San Diego, 2009.

[6] Palka, Bruce, *An introduction to complex function theory*, Springer, New York, 1995.

[7] Pinter, Charles, *Set Theory*, Addison-Wesley Publishing Company, 1971.

[8] Sundstrom, Ted, *Mathematical reasoning, writing and proof*, Second Edition, Pearson Prenticel Hall, Upper Saddle River, 2007.

[9] Schumacher, Carol, *Chapter zero, fundamental notions of abstract mathematics*, Second Edition, Addison-Wesley, 2001.

[10] Taylor, Howard y Wade, Thomas, *Matemáticas básicas con vectores y matrices*, Limusa, Mexico, 1989.

Índice alfabético

Afirmación, 2
Algoritmo de la división, 122, 147
 para polinomios, 155
Antecedente, 4
Argumento, 10
 Válido, 10
Axioma
 de completez, 113
 de elección, 72
Axiomas
 de campo, 88
 de orden, 90

Bicondicional, 4

Campo, 91
 ordenado completo, 113
Cardinalidad, 128
Clase, 47
 de índices, 55
 respecto a una relación, 80
 universal, 49
 vacío, 49
Clases
 disyuntas, 51
Clases y conjuntos, 46
Coeficientes binomiales, 103
Complemento de clases, 51
Composición
 de funciones, 68
 de relaciones, 82
Condicional, 4
Conjugado de complejos, 141
Conjunción, 3
Conjunto, 57
 cociente, 84
 contable, 128
 finito, 128
 inductivo, 98
 infinito, 128
 no-contable, 128
 numerable, 128
 potencia, 58
Conjuntos
 contables, 131
 equipotentes, 125
 infinitos, 131
 no-contables, 134
Consecuente, 4
Contradicción, 6
Contraejemplo, 39
Contrarecíproco, 9
Cota
 inferior, 111
 superior, 111
Cuantificador
 existencial, 17
 universal, 16
Cuantificadores, 16
 con varias variables, 17
 en teoremas, 37

Densidad de los racionales, 115
Desigualdad de Bernoulli, 108
Desigualdades en un campo ordenado, 94
Diagramas de Venn, 50
Diferencia
 de clases, 52

simétrica, 59
Disyunción, 3
División sintética, 161
Divisibilidad, 31
Dominio
de una clase, 80
de una función, 63

Ecuación polinomial, 154
de segundo grado, 154
Ejemplificación
existencial, 19
universal, 19
Elemento mínimo, 100
Equivalencias, 8
Escribiendo matemáticas, 41

Fórmula
binomial, 103
de Moivre, 146
Factor propio, 156
Factorización de polinomios, 155
Familias indexadas de clases, 55
Forma trigonométrica de un complejo, 144
Función, 63
biyectiva, 71
constante, 65
extensión, 65
identidad, 65
inclusión, 65
inyectiva, 71
proyección, 65
restricción, 65
sobreyectiva, 71
Funciones, 63
particulares, 65

Generalización
existencial, 20
universal, 20
Grado de un polinomio, 154

Hipótesis del continuo, 136

Igualdad
de clases, 48
de complejos, 140
de funciones, 65
Imagen e imagen inversa, 66
Implicación, 7
Infimo, 112
Intersección de clases, 49
Inversa, 69
a derecha, 69
a izquierda, 69

Ley
de cancelación, 93
de inducción para enteros, 106
del medio excluido, 3

Módulo de un complejo, 141
Media
Aritmética , 105
Armónica, 105
Geométrica, 105
Meta-Afirmación, 7

n-tupla, 102
Número
negativo, 92
no-negativo, 92
no-positivo, 92
positivo, 92
Números
Complejos, 140
Enteros, 98
impares, 30
Irracionales, 117
Naturales, 98
pares, 30
Primos, 40
Racionales, 106
Reales ampliados, 120
Negación, 4

Parte entera, 115
Pertenece a, 47
Polinomio, 153
completamente factorizado, 157
irreducible, 156
nulo, 154

Polinomios
sobre los reales, 159
Potencias
con exponente entero, 106
con exponente racional, 119
con exponente real, 119
Primos relativos, 43
Principio
de Buen Orden, 100
de inducción matemática, 98
Producto cartesiano, 53
Propiedad
arquimediana, 114
arquimediana de los números reales, 57
de aproximación de supremo, 113
de aproximación del ínfimo, 121
Pruebas
con si y sólo si, 35
directas, 29
por casos, 33
por contradición, 32
por contrarecíproco, 32

Raíces
de complejos, 143
de la unidad, 149
Raíz
$n-$ésima, 118
de un polinomio, 155
Rango de una clase, 80
Recíproco, 9
Reglas de inferencia, 10
con cuantificadores, 19
Relación, 79
de equivalencia, 83
identidad, 80
inversa, 81
reflexiva, 81
simétrica, 81
transitiva , 81
Representación geométrica de raíces
complejas, 148

Segunda ley de inducción, 100
Sistema de números reales, 88
Subclases, 48
Supremo, 112

Tautología, 6
Teorema
de Liouville, 155
del factor, 156
del residuo, 156
fundamental del álgebra, 155

Unión de clases, 49

Valor absoluto, 43, 96